Comparative Analysis of Algorithm For Embedding Information on QR Code

Thesis submitted to the Faculty of Engineering & Technology, Jadavpur University In partial fulfillment of the requirements for the Degree Of

Master of Technology in Printing Engineering and Graphics Communication

In the Department of Printing Engineering

By

Ishita Misra

Exam Roll No. – M4PRI19007
Class Roll No. –001711602006
Registration No. – 140961 of 2017-2018

\

Under the esteemed Guidance of

Mahasweta Mandal

Asst. Professor, Department of Printing Engineering
Jadavpur University, Kolkata – 700098

May, 2019

TO WHOM IT MAY CONCERN

I hereby recommend that the thesis entitled "***Comparative Analysis of Algorithm for Embedding Information on QR Code***" has been carried out by Ishita Misra (Reg. No.140961 of 2017-2018, Class Roll No. 001711602006 and Exam Roll No. M4PRI19007), under my guidance and supervision may be accepted in partial fulfillment for the degree of M.Tech in Printing Engineering and Graphic communication in the Faculty of Engineering and Technology, Jadavpur University, Kolkata.

_____

(Mahasweta Mandal)

ThesisSupervisor

Department of Printing Engineering

Jadavpur University, Kolkata

Countersigned:

1.

_____

(Prof. Soumen Basak)

Head of the Department
Department of Printing Engineering
Jadavpur University, Kolkata

2.

_____

(**Prof. Chiranjib Bhattacharjee**)

Dean, FACULTY OF ENGINEERING & TECHNOLOGY
Jadavpur University, Kolkata

JADAVPUR UNIVERSITY

Faculty of Engineering and Technology

Certificate of Approval

This thesis at an instance is hereby approved as a creditable study of Engineering Subject carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned does not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve the thesis for the purpose for which it is submitted.

Final Examination for evaluation of the thesis

_____

_____

JADAVPUR UNIVERSITY

Declaration of Originality and Compliance of Academic Ethics

I hereby declare that this thesis contains a literature survey and original research work by the undersigned candidate, as part of the Master of Technology in Printing Engineering and Graphic communication studies. All information in this document has been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by thesis rules and conduct, I have fully cited and referenced all material and result that are not original to this work.

Name: Ishita Misra

Examination Roll No: M4PRI19007

Registration No. : 140961 of 2017-2018

Thesis Title: "*COMPARATIVE ANALYSIS OF ALGORITHM FOR EMBEDDING INFORMATION ON QR CODE*"

Signature with Date:

Acknowledgement

I have received the assistance and co-operation of quite no of people during this work on **"*Comparative Analysis of Algorithm for embedding information on QR Code*"** So I hereby take the opportunity to extend my sincere gratitude to all those who have provided their assistance and co-operation and valuable suggestion and time to time in spite of their busy schedule.

Firstly I would like to thank my guide Mahasweta Mandal, Assistant Professor (Dept. of Printing Engineering).She has not only just helped me but provided her valuable suggestion from time to time. I would also like to thank Dr. Swati Bandopadhay Associate Professor (Dept. Printing Engineering & Graphics Communication). I would like to thank Prof. Soumen Basak Head of the department of Printing Engineering and all other faculty members. I would also like to thank the members of Digital Color Imaging Laboratory for their encouraging support and providing me a pleasant atmosphere during my work .

Date:

IshitaMisra

Class Roll Number: ***001711602006***

Exam Roll Number: ***M4PRI19007***

Registration Number: ***140961 of 2017-18***

Department of Printing Engineering

Jadavpur University, Kolkata

Table of Contents

List of Figures

List of Abbreviation

QR code	**Quick response code**
DCT	**Discrete cosine transform**
DWT	**Discrete wavelet transform**
DFT	**Discrete Fourier Transform**
LSB	**Least significant bit**
MSE	**Mean squared error**
PSNR	**Peak signal to noise ratio**
FFT	**Fast Fourier transform**
SVD	**Single value Decomposition**

List of Tables

Abstract

In the digital image processing authentication and copyright protection have become more significant; in order to achieve this digital different watermarking techniques are introduced for the security. Recently the use of QR code for data coding becomes significantly increasing especially for coding identity, health and other specific data in security field. Either the documents are in hard copy or circulated along the web both need equal kind of protection. Main objective of this present study is to combine both QR image and watermarking together to get the higher Robust security feature. The secondary goal of this investigation is to set a best fitted algorithm which can counter measure attacks and compile in lesser time. Two methods are designed and compared in the basis of various comparative aspects like Histogram, comparison based on attacks like noise, Rotation etc. In this study, either DCT-Channel separation method or DCT Block Division Method has been used for designing the security feature. DCT-Channel separation method is applied after dividing the image in respective red, green and blue channel and then applying DCT in two dimensions and in DCT Block Division Method the image is divided in several blocks and a binary watermark is imposed on lower frequency bands as it has the lesser effect on human visual system. Both the methods are analyzed based on normal color image watermarking and then the same binary image is embedded in QR image. The present study has utilized Matlab software R2015a to do the comparative analysis of algorithms for embedding information on the QR code. The common aspect between both methods is that they are dependent upon watermark embedding strength. However the visibility is dependent upon that criteria but quality of both the watermarking process are varies in all aspects. In this study the proposed algorithms are designed scientifically to get a robust privacy protection for new generation of printed and digital media files and to impose better copyright protection. Channel separation and Block division both the methods have some pros and cons though analysis have been done to get the best way.

Chapter 1

INTRODUCTION

As the rapid development of technology, digital information must be protected from threats and attacks such as alteration, deletion, unauthorized modification. Increase in the use of Digital Media, has raised the problem of data protection and authentication. For this reason data can easily be copied. So protecting the data in a robust manner is also a major part in digital image processing. Various kinds of multimedia data like image, audio, video are not safe from different threats while transmitted over the web. Security features are needed to be strong to protect from any kind of interrupts or modification. Digital Image Watermarking is an efficient method to protect digital images from unusual attacks. A watermark is embedded directly in the image to be protected without altering it significantly, this watermark is imperceptible usually, but it can be detected or extracted by specific algorithm, even after some manipulations to the watermarked data. The embedded data (watermark) may be either visible or invisible. To hide the information QR code has been used in digital watermarking process. Providing security by means of QR code is more efficient than password, fingerprints and face detection system. The QR code is a matrix which is an array of square modules arranged in a square pattern. The three corners of the QR code formed a unique pattern that assists easy location of its position, size and inclination. Barcode, QR code and Watermarks are best method to hide secret messages, imposing ownership and tracking elements and many other sectors.

Proposed work is focused on embedding secret information to an image file so that basic ideas of security aspects and image qualities are discussed in details. Starting from very beginning, to the complex algorithms all topics are covered. Protection of a digital media from forgery and prove the owners identity depends upon some security feature The security feature can be applied on the image, audio, video and any kind of text documents. As this thesis is oriented upon digital image only so 1st question arises in our mind is that what is an image and the answer is described in the next section of this discussion.

1.1 Image

An image is a series of signal which can be captured or recorded with a device in different exposure. It is the virtual representation of a live scene. Images are available as printed form or hard copy (Printed form of digital one) and in digital from. Previously printed images are developed through developing the negatives but now that can be printed directly from a digital capturing device (digital camera, smart phones).

1.2 Types of Images

Images can be of two categories they are Raster image and vector image:

A. Raster image: It is a kind of digital image that is created using grids of individual pixels that collectively compose an image. It can be stated that raster images are summation of so many pixel grids where each square is tinted with some particular shade but individually this pixel shows nothing useful only the summation shows a complete image. Raster images are showing

fuzzy edges and these images can be addressed as bit mapped or .bmp image and having so many formats few of them are discussed below.

Fig1: Raster image

i) Tiff: Tagged image file format or .tiff format can be used where each and every details are needed. Tiff format files are very large and flexible in terms of color like they can be grayscale, CMYK and RGB, they are flexible for image layers and tags. .tiff image contains very large number of data because they are uncompressed that's why it is so large in size and each and every details are present.

ii) JPEG (.JPG): It stands for joint photographic expert group. This format of images are designed to store a lot of data in smaller space that's why they are using compression algorithm to create this kind of image files. In time of compression image might loss some information that's why it is called lossy compression. Large amount of compression might degrade the image quality but lower to medium compression is applied to achieve a better quality image in smaller memory space. This format of image are used in web because it can load easily and looks better for both monitor and print.

iii) GIF: It is known as graphic interchange format. It also compresses image data but as different from .jpg the type of compression is lossless thus no information is lost in the time of compression. But .gif cannot compress the image like .jpeg and it also have few color ranges for web and it is not suitable for print. It is never used for photography due to its limited color range it is used for animated pictures.

iv) PNG: Portable network graphics. This format is created to replace .gif format files. .png offer a better compression and wide range of colors than .gif. This type of images are exclusively used in web pictures and not for print. In case of photography it is not as good as .jpeg format but it is useful for images with caption or in graphic arts because the image look less bitmapped.

v) Raw image files: This kind of files are not been processed through any kind of image processing functions. This kind of image depends upon camera characteristics or upon the capturing device. This kind of files cannot be printed or edited or modified by any means thus it is known as RAW image files.

B. Vector image: Unlike the raster image vector images are based upon true geometric primitives. It is used to represent quite smoother images that the raster one there is no aliasing factor near the edges. Vector images are designed with help of some mathematical commands or tools like adobe illustrator coral draw etc. Vector images can be modified easily which we could not achieve with raster image sometime they are converted to vector images to achieve appropriate goals. In vector files no bits are saved they are saved as a sequence of commands which represent the points which should be joint together to reconstruct the whole image.

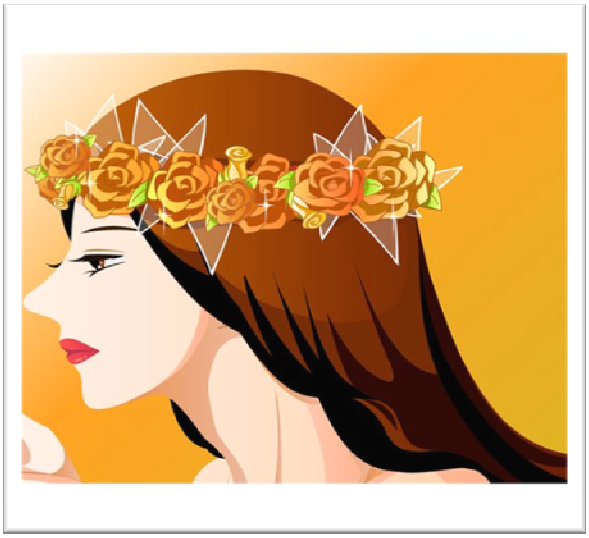


Fig2: Vector image

1.3 Image Quality

As we know that image is a process of capturing a series of signal which represents any live situation through a capturing device and image quality can be referred as the accuracy or similarity between both the captured and the live scene means how similar is the captured image and scene visualized by a human eye (HVS). Image quality is a factor which is mainly dependent upon capturing device and can be determined by comparing various factors like sharpness, brightness, contrast etc. These factors are known as image quality factor.

1.4 Assessment Categories

Image Quality can be measured through some comparative assessment like

Full reference: Here original and test image both are needed to measure the quality

Reduced reference: In this method original image is needed but not in original form it is present there with some distortion like cropped, compressed etc.

No reference: In this method of quality checking no image is needed as reference one.

1.5 Image comparison parameters

Several ways are present to check the basic difference between two images by discussing about basic image quality factors of how two perceptually same images can be distinguished or which one is better and how much difference is present there. In accordance with this paper this factors are deciding the difference between results so they are addressed as comparison parameters. Proposed algorithm uses very few image quality factors and they are described below:

- **Brightness:** It's a perceptual attribute of an image it basically shows the overall lightness or brightness of an image. In this feature source appears to be radiating or reflecting light. It's a visual perception draw out from luminance of target. Image brightness is often confused along image intensity and light ness then we can say intensity is the amount of light energy that is fallen upon a unit surface in unit time. Next lightness and brightness are both perceived terms but lightness is perceived reflectance where brightness is perceived
  luminance.

Fig3: Diffrence in brightness

- **Contrast:** Contrast means the difference in lightness or brightness of an object with the background present in a same image. In other words contrast of an image is the difference of luminance between the image objects which make it more distinguishable than the background. It is the difference between some image attributes like color and lightness of the objects that are present in the same field of view.

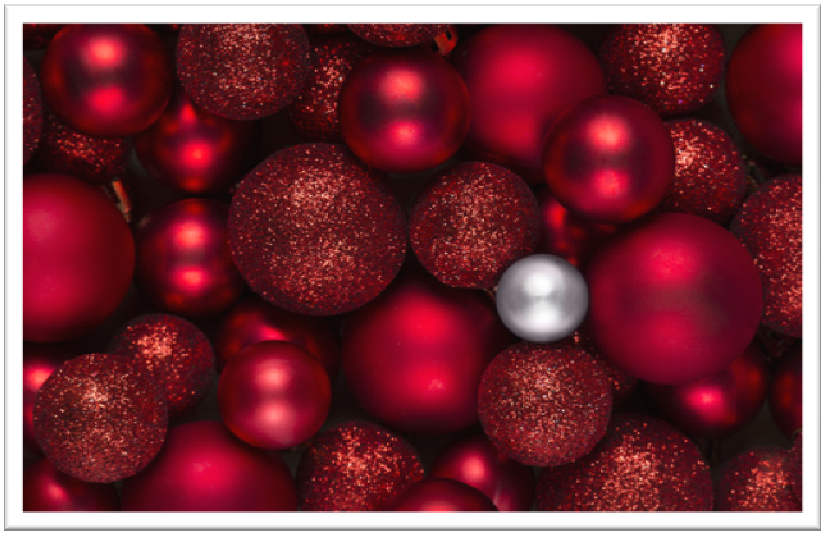


Fig4: Difference in contrast

- **Histogram:** It is like a bar graph structure used for comparative studies it shows tonal distribution of a digital image. It plots tonal distribution for every pixel. Reconstruction of any image from its histogram is not possible, but it can be same for different images. It can solve over and under exposed issues brightness and contrast issues, dynamic range etc. Some basic features of an image can be stated by seeing its histogram or comparison two images by comparing their histogram.

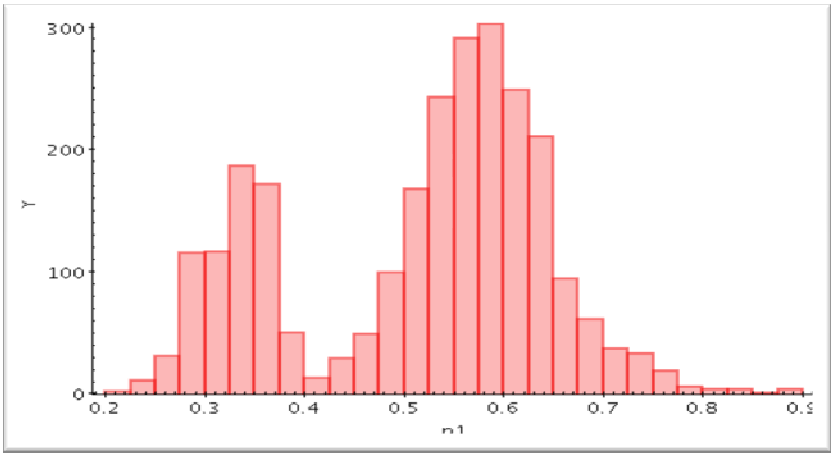


Fig5: Example of an image histogram

1.6 Objective of the work : The goal of this study is to find a robust method for image and QR image watermarking. Comparing and analyzed the two different algorithms: DCT channel separation method and DCT Block division methods to check the efficiency of algorithm among them for watermarking process.

1.7 Scope of the work: This work is basically oriented upon the security features of printed and soft documents. In this process mainly 3 protection features are used 1.Barcode, 2.Watermarks, 3. QR code. Various kinds of work has been done upon this topic. Lot of researcher has done their work in any one of this features. Main attraction of this paper is combining two security methods applying two different algorithm and try to analyze the best method for further work. In our work we have combined both the Watermarking and QR code using discrete cosine transform, but we have applied DCT in both the cases in two different manner for the 1st method we applied DCT on image blocks and in the 2nd method DCT is applied upon the image channels. Comparing the results of this two methods conclusion can be drawn on which one is more suitable to get more robust and secure results. It can help in ii) getting a reliable and robust feature that can hide information about any kind of package, Documents, multimedia data and so on.i).saving time. For this reasons this algorithms will help in media industry as well as in printing and packaging industry. It has a wider range of application from small organization to bigger one this can be helpful to protect their data's or keep track of their data, it can be useful in stock management also. iii)this process can analyze which method is more time saving and more easier so that researcher can get a help to impose more number of security features in a much lesser time. Proposed work applied not only in digital transmission but also it can be used in vast area of printing and packaging industry to check authenticity and security of the product.

CHAPTER 2

LITERATURE REVIEW

This chapter presents a literature review on relevant embedding information system on QR code. It explains and critiques related work studying and choosing the appropriate practices used to enhance security features. It also discusses the fundamental properties through which embedding information systems are evaluated and asserted. Watermarking is a technology which will impose property rights to a digital media files like audio, video, image and in many cases on hard copy of any document. It is inserted into a media (audio, video, and image). Process of insertion and extraction follows various algorithms. There are 2 basic characteristics of watermarking they are Robustness, and Imperceptivity. These two measure majorly decides how good the watermarking is. There are various ways to take action on the security perspective of a digital or printed document in this review discussion is made about some existing algorithms and what are the advantage and disadvantage of them.

Zhang Y. [1] has explained the Digital Watermarking technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. The characteristics of the watermark like imperceptivity, security, reliability, low complexity of watermarking algorithm and security of the hiding place applied for embedding, extracting, error correction is discussed. The basic characteristics of digital watermark is. Digital Watermarking Algorithm is composed of three parts: watermark embedding algorithm, the watermark extraction algorithm and the watermark detection algorithm. Future research of digital watermarking technology will focus on the watermarking algorithm, the study of watermarking theories, the watermark attacks and the evaluation system of watermarking system.A theoretical model of digital watermarking is demonstrated in which it is divided into 3 section of algorithms that should be used while designing a whole watermarking system. The **Embedding Algorithm, The Detection algorithm, The extraction Algorithm.** Author has also discussed about three other lesser known algorithms named as "Patchwork Algorithm" earlier this algorithm is used for security of printing bills the 2nd one is the Direct Sequence spread spectrum Algorithm and Text minitrim and texture mapping algorithm. The error detection algorithm like Mean squared error (MSE) or peak signal to noise ratio (PSNR) is also presented. The further research work is directed.

Mistry D. [2] has described the comparative studies between all the possible embedding methods and mentioned that the simplest way of watermarking is LSB watermarking. In LSB method, it uses the least significant bits of the cover image to hold the hidden message because human visual system is not very used to notice very small difference of colors. The embedding process is shown applying LSB where the RGB image is converted to gray scale and made double precession for the image and the most significant bits have been shifted to the LSB bits of the watermark after that LSB bits of the cover image has been changed to zero and the shifted version of watermark image is added with the improvised version of host image. Additionally, the limitation of this algorithm has been reported. In further discussion author has demonstrated the DCT and DWT both the transform domain algorithms. In DWT for the encoding part

division of the image into 4 frequency bands is done and after that applied Haar wavelets at the 1st level in 2nd level image is segmented on 7 frequency bands and again Haar wavelet is applied and the process is going on. After this step a pseudo random sequence N is added to the high and medium frequency zones. The normal distribution method is applied to achieve robust against all attacks. The weight is added to the watermark according to the weight of wavelet co efficient.

$$\bar{y}_{ij} = y_i + \alpha \cdot y_i j^2 \cdot N_{ij}$$

$$\bar{y}_{ij} = y_{ij} + \alpha \cdot |y_{ij}| \cdot N_{ij}$$

These two equations are used as the main embedding equation using wavelet transform where α is the control level of watermark and y and ȳ are the co efficient of the host image and watermark respectively.

Ingemar J.[3] also focused on Application and properties of watermarking methods where a number of applications of digital watermarking are discussed. Moreover, the common properties of robustness, tamper resistance, fidelity, computational cost and false positive rate are investigated. The study is concluded with a remark that evaluation of any watermarking algorithms is not possible without mentioning the context of application. It is also mentioned that watermarking is a technology which can serve a wide variety of applications, each of them may have very different requirements. Moreover a single set of standards should not be applied to all proposed watermarking systems. Different set of standards should be applied to each system according to the application for which it is intended.

Jiansheng M et. Al [4] have proposed a discrete wavelet transform (DWT) digital watermark algorithm based on human vision characters. The watermark image has been discrete cosine transformed in order to increase its robustness as it has contained the low frequency information of watermarking image. By applying the block technology, watermarking signal is embedded into the high frequency band of wavelet transformation domain. The proposed system has showed that this watermarking system not only can control the image quality well, but also can be robust against many common image processing operations of filer, sharp enhancing, adding salt noise, image compression, image cutting and so on. Also it shows a strong capability of embedding signal and anti-attack.

In initial stage of the work DCT is applied in the image and it is known that DCT has the low frequency information so the minute destruction can't be notified by human visual system hence it will give better robustness and imperceptibility. Basic 2 dimensional DCT equation is used because the image is a 2 dimensional matrix. The whole embedding process is explained as, At 1st the 2 dimensional DWT is applied to the host image after that wavelet co efficient of higher frequency band has been selected then the streak block has been chosen and the DWT image has been divided to 2*2 sub blocks, the entropy and the square value of the each sub block is calculated and the lowest value of entropy is been considered as the smooth block and the bigger

value of image is been considered as the edge block or streak block. In the last step of embedding 2 dimensional DCT is applied on the watermark image and spectrally distributed image is obtained. For embedding the below mentioned equation is used.

$$C'_k = C_k + \alpha * V_k, \text{ k=1,2.....} P * Q$$

where C_k is considered as the wavelet co-efficient , V_k is the no of watermarking component weight of sequence V, and C_k is the new co-efficient value of streak sub block U_k it represents the wavelet co efficient value of the streak blocks, a represents the embedding depth of the watermark. The inverse transform is applied to the combine image to get the complete watermark image. Simulation had been done in the Matlab 7.0 using the grey level image of Lena (256x256) as the host image and another 32x32 binary image as the watermark image. A new term watermark distilling is presented which basically means the extraction procedure by using entropy calculation.

Kutter M. et al. [5] have proposed a new version of watermarking process in order to make more robust watermarks. The digital watermarking schemes of new generation is using pixels, frequency or other transform co-efficient to embed any information. The main drawbacks of this schemes are that the watermark is embedded into non-significant part of the data. Authors have mentioned such techniques as first generation watermarking schemes. Proposed Algorithm focused on second generation watermarking schemes. First generation watermarking schemes, employ the notion of data features but the proposed work is based on point features in images using a scale interaction technique based on 2D continuous wavelets. The features are used to impose a partition on the image.Spread spectrum technology to embed the watermark inside an image basically two basic steps are applied to find out the image feature reference location to embed spread spectrum modulated watermark and then. The images are segmented according to the feature point using 2 Dimensional Mexican hat wavelet. It is described that this two point in detail in the further part of the paper. About the feature point they have added that features points which are detected in manner that they can put up with all sorts of geometrical distortions like rotation scaling and cropping. Feature extraction of this algorithm based on Mexican -hat-Mother wavelet transform also known as Maar wavelet they consider at location (x) the wavelet function x is two dimensional direction co-efficient of pixel. It is explained that these schemes are more robust to attacks when they are designed and as long they can't degrade the commercial value of a watermark the watermark is not visible to HVS.

Spread spectrum technique is a process of passing narrow band signal over a much larger one. It took the basic idea from the communication channel theory. They consider frequency domain of the image as communication channel and using spread spectrum technique transmit the watermark over the communication channel. A number of images are watermarked using a benchmarking tool called Stirmark. This tool performs various attacks on the watermarked images. The obtained results have shown the strengths and weaknesses of using Cox's algorithm with varying composition images as a cover media. Here it is considered that N1 and N2 are the

height and width of the image and b is the matrix co efficient of the dct matrix watermark, A (i, j) is the intensity of pixel in row i and column j .DCT always uses real multiplication. A new term watermark embedding strength is introduced. It has greatest effect upon imperceptibility of watermark. A scaling parameter α is used as strength co-efficient this spread spectrum based watermarking technology is also known as 2nd generation watermarking algorithm author uses stirmark benchmarking tool for simulation of this algorithm. Two images are watermarked and attacked using this tool and two images shows different result 1st image leena.jpg is a smooth image with lot of similar colored regions and 2nd image baboon is a rough image with lots of color variation. results shows that 1st image is not showing so much variation after applying low pass filtering another image shows effect on low pass filtering. Remark can be drawn that Cox watermarking algorithm are showing better results in smooth images than the rough images because DCT coefficients are used to embed the mark. These coefficients are embedded in the most significant areas of human perceptivity like large area of similar color or repeating pixel. [6]

DWT-DCT watermarking algorithm is purely discussed only on simplest way to get the robust watermark [7]. DWT is applied in the initial stage of embedding and DCT after that. 4 level DWT is applied on the host image to help them broken up into low and high frequency blocks. After that Two dimensional DCT has been applied to the resultant wavelet transformed image. In this step watermark and secret key is been embedded into the middle and lower frequency bands of the host image and after that inverse DCT and inverse DWT is applied and the newly watermarked image is achieved. After that extraction process is described which is completely based upon the inverse DCT but in between these two step description is given about the attacks and the effect of them into the host image. In this work main objective is to hide handwritten signature or phone number inside the host image. So this watermarking should be more robust in nature as they hide more information than the pseudo random codes. Encoding of watermarks is done before it is inserted in the still image; embedding process took place in frequency domain rather than spatial domain.

Different kinds of watermarking process are discussed depending on image watermarking[8]. It also included the categories of watermarks **.**Pseudo Random Gaussian sequence is a sequence of number 1 and -1 which are considered as watermarks having equal number of 1 and -1.these are created with zero mean and one variation and used in object detection method. Binary image or gray scale imag**e** Instead of a Gaussian sequence black and white logos are used as the watermark this kind of watermark is called the Binary image this watermarks are used for subjective detection. Based on the embedded watermark the embedding algorithm and extraction process is been chosen and the process of detection is also determined like if the embedded watermark is a Pseudo random Gaussian sequence according to the algorithm the Bit Error Rate method is used to test the presence of watermark like if the Bit sequence of watermark is W and the extracted watermark is W' and BER is zero then the watermark is present and if the BER is one then the watermark is missing in the host image. Calculation method of Bit Error Rate is

$$D = \begin{cases} 1 \ if \ W_i \neq W_i' \\ 0 \ if \ W_i = W_i' \end{cases} \qquad BER = (W, W') = \frac{\sum D}{N}$$

Normalized Correlation Coefficient is also used to recognize the presence of watermark.

$$NC(W, W') = \frac{\sum W W'}{\sqrt{\sum W_i^2} \sqrt{\sum W_i'^2}}$$

The work also described about a detailed survey about watermarking technology in which manner the previous works has been completed, and introduced a new method that is watermarking based on perceptual modelling which means embedding perception of the watermark should be based on which method the author of this paper categorized the previous research work in the basis of No perceptual modelling, Implicit perceptual modelling and 3.Explicit perceptual modelling. In the first category there are no such perception is used (Noore, Fotopoulos and Skodras) in this methods. In the 2nd option that is implicit modelling the authors used transform domain properties for perceptual modelling which can use the co-efficient selection method in which researcher can choose the highest transform domain co-efficient which can hold the higher perceptual capacity which means it can allow stronger watermarks which have least perceptual distortions. In the 3rd description is given about explicit watermarking which means they are embedded depending upon the HVS properties it also consider the basic properties of an image like brightness contrast scaling etc. After this section author discussed about the DCT and DWT watermarking and their advantage and disadvantage, Blind, Non blind watermarking methods, a survey on how many works have been done based upon DCT & DWT algorithm. The main objective of this work explanation is given about DFT Algorithm and the advantage of DFT over DCT and DWT according to work the main advantage is that DFT is rotation and scaling invariance. DFT can be categorized in direct embedding and Template based embedding which is proposed by Pereira and Pun (2000) watermark which is resistant to affine transformations.[8]

Saini L. et al. [9] have the discussed about basic theoretical aspects of watermarking. Discussion covered the Performance evaluation algorithm MSE and PSNR. MSE can calculate the mean squared error between the cover image and the watermark image using the equation

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

Where MN is the pixel in the cover image $I_{i,j}$ is the pixel of watermarked image and $K_{i,j}$ is the pixel of host image. The 2nd algorithm is peak inverse signal to noise ratio can be calculated by

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

Where P is the highest value of the cover image and author also included that the imperceptivity of watermark is dependent upon PSNR value. Apart from the commonly used DCT, DWT and spatial domain algorithm there are two new kind of algorithms which are also used for watermarking algorithm . Two new term is came to sight one is the 'Ridgelet' transform based digital image watermarking and CDMA based Spread Spectrum Digital. Ridgelet transform is the next generation wavelets which are performed best in 1-Dimensional wavelet transform. Mathematically continuous Ridgelet transform is the combination of radon transform and 1 dimensional wavelet transform in a schema author showed that if Radon transform is applied to the original image and then one dimensional wavelet transform is applied the result will give the Ridgelet transform it can be given by this series of equation like

$$CRT(a,b,\theta) = \int_R \psi_{a,b}(t) RDN_f(dt) \, , RDN_f(\theta,t) = \int R^2(x,y)\delta(x\cos\theta + y\sin\theta - t)\,dx\,dy$$

Where 'a' is scaling parameter, b is shifting parameter and θ is rotation, R2 indicates real line. It is efficiently used for image compression and application in robust watermark embedding can also be done. [10].

In accordance with other presented algorithms the basic idea of watermarking features and properties is are investigated. The comparative study of basic working principle of watermarking and steganography are discussed. It is added that primarily they both methods are doing the same work (to hide a message) but the main difference is that watermark hides a message which has a relation with the actual carrier signal but for steganography it only acts like a cover signal which didn't carry any relation with the actual message signal. Discussion is made about different kind of watermarking models which can be considered as the new field for further work. The watermarking methods are divided into Geometric models and Communication based models. Geometric model is that in which Geometric models images are considered as vectors of high dimension in a media space where images of all dimension are present. Geometric models divides the watermarking process into several regions. one of them is e*mbedding region* where all the possible images from embedding of secret data into a cover image is been present and that are embedded using some watermark embedding algorithm. Another part is *detection region* in this part all the possible images are present from where the watermarks can be extracted using watermark extraction algorithm. The last part is the *acceptable fidelity region* where all the possible image from watermarked image is present which looks like the original host image. [11]

Lots of research already has been done upon Digital image watermarking. Several algorithms are concentrated in different domains like embedding and extraction methods based on various algorithm ,in performance evaluation. The discussion is summed up the improvement of first 50 years of Digital image watermarking. Moreover, digimarc has been discovered a class of device that links the traditional printed documents with media [12].

The visible and transparent both watermarking methods are presented. It is reported that the visible watermarks do not count the capacity criteria of the host image transparent watermarking

can be of three types 1) fragile 2)semi fragile 3) Robust, description is given about Document, Video, Audio and Graphics watermarking along with the image watermarking . The main criteria about watermarking is that no significant noticeable difference should be present in between the watermarked and host image. The watermark should not be removed or alter easily. [13].

Anan T. et al[14] have proposed two watermarking technologies named watermarking for copy control, anjd watermarking for traceability. The two methods like background texture type and font embedded type are utilized in the development of these two techniques. For the 1^{st} type the secret data is embedded in the tint-block background of a hard copy (printed copy) this kind of patterns are addressed as starlight patterns in real means the stars are the hole in which manner the secret message is embedded to it. This kind of feature has an extra advantage that is it can give up-to 10^{th} generation of copy protection another features are it considered as high secure pattern. Now the 2^{nd} point is font embedded type in this kind the watermarks are inserted by changing the shapes of the character.Moreover, the documents which are processed using this technology has no background texture and uses the binary image, alpha-numeric codes as security information etc. The watermarking for copy control can be implemented to differentiate an original from a copy .The watermarking for traceability is applied to embed the information secretly about a person who prints the document indicating the source of information. These two methods can be applied individually and integrated with existing security system to protect printed materials.

Mettripun N. et al[15] have developed a new watermarking scheme based on the modification of image pixels in order to improve the accuracy of the extracted watermark and the robustness of the embedded watermark. These techniques are applied for both color and grayscale images. A robust image watermarking technique based on a modification of the luminance component of the host color image is presented. Three methods are demonstrated in the watermarking scheme in order to improve its performance in terms of accuracy of the extracted watermark and robustness of the embedded watermark. These methods are a new scientific approach to watermark embedding in the luminance component of a host image and a new original image prediction technique in the watermark extraction process. A set of experiments is performed to verify the recommended methods. *In Luminance Modification* , luminance components are used in spite of the color components . An explanation stated that general image compression can affect the chrominance factor of the color image because of the subsampling process.so use of the luminance modification process for embedding the watermark shows more robust results against compression attack than the color component embedding's. Work includes YC_bC_rColor model for the embedding process where Y is the luminance component and C_b is the chrominance of blue component and C_r is the chrominance of blue component. Though human visual system is very sensitive to luminance change so changing in Y may result a severe effect on the image. To overcome this situation author has reduced the number of embedding bits to decrease the effect of watermark image bits in Y component and similarly it improves the

quality of watermarked image this solution is choosen because it doesn't affect or degrade the size and quality of the image. It used the PSNR equation [9] to show the quality degradation after watermarking. After embedding as a difference to other methods the author uses the term reconstruction of watermark where the DWT algorithm and three steps to create another watermark. For the new watermark 1st two processing steps are dependent upon 2D DWT and reduce the size of hidden image and increase the size of extracted watermark image, last step is for DE noising the extracted image and remove the negative consequence of propagation error. In the last section of this work a comparison is done between 5 major watermarking methods which uses luminance modification method in their algorithm.The significant improvements are achieved utilizing the watermarking scheme compared to previous existing schemes. After application the method, the results have allowed to improve the enhanced robustness of the embedded watermark against various types of attacks.

Jimson N et.al [16] have proposed a watermarking algorithm which is purely based on DFT. It is known that DFT based algorithms are rotation and scaling invariant. Mainly, a brief theoretical background of the DFT and some common terminology are discussed in digital image watermarking. It is stated about some new kind of attacks like removal attack in this type of attack mainly the quantization, compression, demodulation, denoising. this kind of attacks took place which means the attacks which are capable of removing the watermark from the watermarked image without using the key encoded to them are part of this category, though this kind of attacks are considered to remove the watermark completely but they couldn't do it completely but of course they can affect the watermark partially. In protocol attack ,the attack is applied upon the whole watermarking system mainly the party who are embedding watermarks can apply this kind of attacks in the system to impose false ownership according to the author this problem can be overcome by creating the whole system one way functional and signal dependent, Copy attack is a kind of protocol attack because here also the attacker assume the amount of watermark and used it into another digital data. In geometric attacks in this category geometric distortions like rotation, scaling, cropping etc can took place in accordance with this publication this kind of attacks can overcome by Fourier Mellin transform which is also known as transform in variant domain, specially designed auto co-variance function (ACF). In cryptographic attacks, this attack have high computational complexity oracle and Brute force attacks are known as cryptographic attacks. These are measured while embedding the watermark into the image and finding out the process of removing the marks or inserting another misleading part in the watermarks. They have discussed to cover the details of the watermarking algorithm based on DFT. The DFT based watermarking scheme is invariant to RST attack in compared to other transform domain watermarking like DCT, DWT. DFT based image watermark scheme can be classified into template based approach, circular embedding using some radii.

Delaigle J.F. et al. [17] have represented all watermarking models particularly based on Human visual system the main motto of using digital watermarking method is to use them all in a way that they are not visible to human eyes or embedded in such a way that it couldn't be

distinguishable through the naked eyes. So discussion is made about the perceptive model which describes the phenomena of masking by which it can be measured that how well the watermark is hidden. The applied technology is divided into many steps like eye functioning and masking concept in which it is stated that retina and eyeballs are splitting the signal components of an image in several parts which are received by them. According to their characteristics they passes separately from retina to cortex using separate channels the components of same characteristics are tuned to same channel so the component which are belong to same group must have same location in the visual field, same spatial frequency and same orientation. So according to the human perceptive model same channels carry the signal of similar components. Proceeding to masking method than it took place when a signal can't visible due to another signal of near characteristics in higher level. The masking model is created on monochromatic signals and in signal with one orientation and single frequency (f_0,θ_0) which is also known as gratings**.** A new concept of masking criterion is introduced because the masking method only focused around gratings to reduce masking criteria of any real image this new technique is introduced to take care of the prior masking condition. The main method of this paper is to embed a copyright information through a binary code into a grayscale image without degrading its quality. For this author uses MLS (maximal length sequence) to encode the secret binary message this MLS has good co relation characteristics and this auto co-relation factors has higher value than the cross co relation factors (co-relations are the factors which are made with shifted version of a sequence). Another main criteria of embedding is the above mentioned masking phenomena. It assure the invisibility of watermarks and the bits which is to be embedded are calculated form the co-relation factors. According to work main attraction of this algorithm is using the visual perceptive model to generate an invisible watermarking model.

A secured watermarking methods using discrete cosine and discrete wavelet transform are described which can be used for the data validation[18]. The secured digital watermark is added by the hybrid method for which a combination of discrete cosine transform (DCT) and discrete wavelet transform (DWT) methods are utilized along with cryptographic technique (Arnold Transform). This technique provides strong robustness and perception transparency to the watermarked image and original image against different kind of attacks like cropping, noise and scaling. Furthermore, the results are compared with Least Significant Bit and Discrete Cosine methods.

Yang Y. et al.[19] have discussed watermarking procedure which is based upon Discrete cosine transform (DCT). It is stated that DCT is the better watermarking algorithm and robust against any kind of noise attacks. In embedding part they divided image into non convergent blocks and applied DCT in each block. A grayscale image is used as host image and a black and white binary image as watermark. Embed the watermark at lower frequency zone of cover image using the equation of watermarking embedding strength $\mathbf{V_i=V_i\ (1+\alpha)}$. It is included that Matlab is a better tool for image watermarking method and this method is quite easier and improvised than the traditional codes.

Yang Y. and Haiping L.[20] have discussed a kind of DCT algorithm, and the code of embedding, extraction and attack based on Matlab. Then the simulation experiments are carried out in Matlab as it proves an efficient tool. The watermarking method using DFT domain watermark which is embedded have circular symmetric property and correlation is used for detection method and it's a blind detection method. This algorithm is designed to show that along with the various attacks it should not degrade image quality if there any alteration of the watermarks is took place. In the time of embedding it is pointed that Circular shifts in spatial domain will not influence the magnitude of Fourier transform and rotation in spatial domain will cause rotation in frequency domain. Embedding using DFT will have zero mean value because it consider 2D sequence which take only 1s and -1s values and as the number of 1s and -1s are same will convey zero mean. In this method watermark is embedded in the middle frequency zones because improvisation in lower frequency zones will cause a visible effect in spatial domain and compression will affect higher frequency of Fourier transform.

S. Agreste[21] has focused on preprocessing of digital image watermarking using wavelet transform. Both the HSV color transform and wavelet transform is applied in combined manner and this the main strength of this algorithm and other than any other algorithm using wavelet transform is the pre-processing step in this stage square, rectangular input images are taken not only this different dimension and different size of input images are also acceptable. DWT can generate matrix of order power 2 as of the input image it happen in pre-processing step of this algorithm and it works in both embedding and detection method. This is a non-blind watermarking process so that it embeds the watermarking algorithm in higher frequency domain. In this method pre-processing step is very important and if there is too much difference between both the image than they are divided in two parts and dwt is applied on both of the image blocks. After generating the new matrix the value plane matrices are used as value planes of HSV models. At time of detection process a new step is introduced which is known as Synchronization step. The watermarked image is different from the original image in pixel, dimension or may be differ after introducing attacks like rotation, scale, crop to it. Main work of this synchronization step is to make same dimension of both the images by using the value statistics of both the matrices. The main advantage of this work is to make more robust and imperceptive watermarks and reducing the probability of false positive and false negative errors by using Neyman-Pearson statistic criterion.

In the previous works lots of discussion have been done upon various algorithm which are used in watermarking procedure, maximum uses of transform domain algorithm has been mentioned and most popular among them is DCT (Discrete cosine transform) and DWT(discrete wavelet transform) the basic work of DCT algorithm has been described. Algorithms are applying to DCT Method for removing block artifact from the compressed image. DCT is applied on an image and inverse DCT upon that to reconstruct the image because by applying 1- D DCT images are divided into spectral sub bands. To get best results quantization matrix is applied and increase the number of quantization matrix until the best result is achieved [22].

Barni M. et al.[23] have suggested a new watermarking algorithm for digital images in which the method, which operates in the frequency domain, embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. After embedding, the watermark is adapted to the image by exploiting the masking characteristics of the human visual system, thus ensuring the watermark invisibility. By exploiting the statistical properties of the embedded sequence, the mark can be reliably extracted without resorting to the original uncorrupted image. The methods like unobtrusive which means the mark is perceptually invisible and quite difficult to effect its quality and readily extractable which defines that the mark can be easily extracted by data owner**.**. In this work it is demonstrated that a watermarking in frequency domain can consists of 3 steps Image transformation, Watermark casting and Watermark recovery. The watermark casting is done 1st then the watermark detection after that theoretical analysis and last of all they have done Visual Masking. In 1st part they have taken a NXN greyscale image and compute images DCT co –efficient as I and store it in a zigzag manner (like .jpeg compression). It includes some differences from cox algorithm [5] which is that decoder can't determine the largest magnitude, original image is no longer available for comparison and the mark is always inserted in the same set of co-efficient. The results show that the watermark is robust to several signal processing techniques, including JPEG compression, low pass and median filtering, histogram equalization and stretching, dithering, addition of Gaussian noise, resizing, and multiple watermarking.

This is the 1st work presented where discussion is made about SVD based watermarking which means watermarking based on single value decomposition. According to the proposed algorithm user can increase invisibility of watermark and increase capacity of watermark while embedded in the U and V component inspite of embedding the watermark only in U component.Capacity and PSNR value of embedded image is calculated to show the result which meet the objective[24].

After application of SVD algorithms, the resutls show some feature like they would have same non- zero singular values in the time of flip, rotation, transpose, translation. Scaling factors have been chosen from a wide range of LL zone. In other words DWT based watermarking method LL bands are not preferred because they may affect transparency of watermark but it is proven that the DWT-SVD based method have not shown any kind of degradation upon watermark quality. It also stated that HL and LH band are good for histogram equalization and gamma correction but it can't resist cropping attacks. In another section normal SVD based method is shown and proposed scheme shows that DWT-SVD has better robustness and reliability[25].

Presented work is based on combinational watermarking scheme of Visual cryptography and Discrete Cosine transform It is stated that in this proposed method two shares of visual cryptography is created and one of them embedded in color image and other is protected by copyright. In the 1st part of the work given a brief details about visual cryptography and DCT algorithm. As per the design of the following watermarking scheme is divided embedding

process in few steps at **The pre-treatment:** when position of the watermark is chosen they should be embedded in a part where human visual system is not so sensible. As blue component is least sensitive to human eye. **.. The embedding process:** At 1st watermark (S) is processed to generate two shares S1 and S2. Basically it used binary image as watermark and XOR based algorithm to divide it in S1 and S2. After this separated blue component image is divided in to 8X8 sub blocks. Then DCT is applied to each sub block and DCT co-efficient matrix Y is generated.S1 is then embedded to the blue component image and S2 is protect by copyright and will be used in time of extraction. Inverse DCT is applied to the whole combined image and by analyzing three colors color watermarked image is obtained. In the extraction process all the steps are repeated in a reverse manner and at last S1 and S2 is combined using that XOR based algorithm so that they achieved watermark and original image individually. After this embedding and in time of extraction some attacks is applied and showed the effect of that on both the images. [26]

In this proposed algorithm discussion has not involves any embedding or extracting methods discussion is about various kind of attacks and especially upon rotation and scaling which algorithm is suited well for this kind of attack has discussed. At 1st watermarking based on magnitude of Zernike moments technique is described. This methods is supposed to invariant in rotation and scaling. Zernike moment is a technique which is used in image processing application because it shows rotation invariant property and in 2nd part author proposed an algorithm based on DCT (proposed by Y.et al.) which is not rotation invariant. In 1st technique the watermarks are embedded in the cover image using modification bits of Zernike moment. The real values are only considered by watermarked image function imaginary parts are put zeroes [27].

The geometric distortion and halftone in print-and-scan process is analyzed for the sake of presenting a model of print-and-scan. A digital watermarking countermeasure method is described [28]. In case of soft copies there must be some effective algorithms but some time it fails to give an appropriate result while printing or scanning the image for that this algorithm is proposed method is effective for ID card printing and scanning, batch coding where the watermarked data obtains a square area. In first part of the work describes hardware models of Printer and scanner device and then started the process of detection watermarks using some basic steps like preprocessing, detection and correction steps are included. Here the ID card suffered some distortion while printing or scanning like not placing properly, edge not detected, blur etc has been noted in preprocess step. In detection step basic summation is done to found the detection workflow and in correction process interpolation is used to recover the errors. Remarks can be drawn that this is the simplest algorithm for countermeasure watermarking process basis of print scan models and also added that different printer and scanner device and different printing process will show differently so algorithms should be designed accordingly. The results have ensured the efficiency of the proposed watermarking countermeasure. These methods may applied in the field of copyright protection and anti-forgery for paper media.

Lin y C.et al. [29] have proposed an algorithm which is resilient against rotation, scale and translation. This method is chosen because many of the watermarking algorithm still now is not so robust against geometric attacks like rotation scaling cropping etc. In this process, Fourier transform is applied on an image and embed the watermark into the obtained one dimensional signal form the original image. Then resample the Fourier magnitudes in log polar co-ordinates and along the log radius axis the summation of resampled values have been placed. It is observed that for rotation extracted signals have faced a cyclic transform, scaling will increase amplitude of extracted signal and translation will not affect extracted signal by any term. So they applied simple search algorithm for rotation, and for detection of scaling they used co relation co-efficient. Remark is that this algorithm can give a better result for cropping attacks also. 1st they divide the image in few overlapping image blocks and then this RST algorithm is applied on each block and averaging all the blocks results has given a better crop resistance also.

This proposed work is focused around a rotation scale invariant watermarking method but unlike [29] previous algorithm it doesn't count any conventional algorithm directly inspite of that this work used higher order spectra or a particular bi spectrum vector of original image. It is mentioned mentioned that higher order spectra is nothing but triple co-relation function of a 1D signal which is obtained by applying DFT on original image . Integrate the bi spectrum vector and phase of this vector will results in a scaling invariant property of this algorithm then they applied Rodon transform and rotation invariance is achieved. To achieve invariance against other geometric attacks, Jpeg compression, Gaussian noise attack image is divided in 1D projection and created a feature vector and then the watermark is embedded by modifying this vector and calculate the distance between new modified vector (after embedding watermark) and the feature vector form the host image and it can remarked that results are showing better invariance against various geometric attacks.[30]

Wang Z. et al. [31] have proposed a work entitled as "An effective watermarking method against valumetric distortions" shows that many quantization based watermarking methods are capable of handling any one kind of valumetric distortions but in this work a watermarking scheme is proposed which can tackle three kind of distortions at the same time. In 1st part of the algorithm related work is divided into four categories a) Estimating amplitude scaling parameter b) Using spherical code words c) Adaptive quantization step d) constructing amplitude scaling invariant feature. As per presented method it is stated a projection based method which satisfies some constraints they constructed a constant change invariant domain using spread transform where watermark should be embedded. Watermark is embedded using amplitude scaling invariant method. Four type of algorithm and different type of attacks has been implemented upon the proposed method to check its effectiveness and in as remarks it can be stated that their method has better gamma correction, better for constant change attack and some time it can resist common image processing attacks and influence a little to the original image.

Wu D et al.[32] have proposed an algorithm which represents watermarking scheme which is resistant to print scan method. Previously mentioned all the discussion are mainly based upon

watermarking embedding and extraction imposing attacks in digital domain but for this paper the discussion included watermarking embedding and extracting and problems during hard copy transfer. It used simple wavelet transform but along with radon transform. In this proposed method other than watermarking image hashing is used to some extent it is better than normal watermarking method in terms of robustness it will give more robust watermarking because normal watermarking the data invisibility is restricted by embedding strength. Image hashing technique would not attract any kind of malicious attack like normal watermarking.The proposed work has few segments at 1st they discussed about properties of Radon transform under some geometric attacks and luminance change than they described about their work. Attacks are divided in few categories by them 1) attacks which can change individual pixel values like filtering and adding noise. 2) Attacks which can change the values of every pixel uniformly like luminance adjustment 3) and geometric attacks like scaling and rotation. As whole the radon transform has been applied in an image which is divided into equal 400 blocks .After the calculation of the mean value of each block 2 level haar wavelet transform is applied to each column and Fast Fourier transform is used to the high frequency co-efficient then only the real parts are considered in the calculation of creating hash string. It is stated that the algorithm can be used to increase robustness and discrimination between the original image and print scan copy.

Watermarking using different kind of algorithm under various attacks have been discussed in which the combination of rotation and scaling are also reported[29,30] . But in this method Fourier-Mellin invariant based transform has been used for watermarking and concluded that it can't affect the watermark under any kind of geometric attacks like rotation, scaling, translation, cropping etc. This is a blind watermarking technique because original image is not required for analysis. Fourier transform is chosen because it has some basic properties like translation property, reciprocal scaling property, rotation properties etc. Using Fourier Mellin transform to get RST invariant property at 1st fast Fourier transform is applied to original image than on the amplitude log polar mapping is done along with this step in phase inverse FFT applied after log polar mapping again FFT applied to the resultant amplitudes and in phase part IFFT applied. From amplitude part we can get the RST (rotation scale transform) invariant feature for watermarking.[33]

The rotation scaling invariant watermarking method is proposed that can allow the recovery even after various geometric distortions and it can allow the same watermark to embed multiple times in the host image at different position. In this method the watermarks are given by a binary number and each and every number is represented by a 2 dimensional function. In proportion with luminance a mask is created the functions are weighted according to this then the watermark is modulated to blue component. Because it has the least effect on human visual system. [34]

Borg A. et al.[35] have shown the process of embedding digital signature into an image. It is demonstrated that an invisible identification code that should be permanently embedded within

an image and should be resistant of any kind of attacks. The whole DCT algorithm is divided in two steps where the 1st part allows the 8X8 blocks pixel in equal distance using Gaussian network classifier and in 2nd phase pixel selected previously are used for embedding along with DCT co-efficient. As a brief two techniques are used for embedding one is called embedding using linear detection constraint and another is embedding in circular DCT detection domain. By using these methods a watermark is designed which is robust against normal image processing attacks mainly the image compression attacks.

LIN et al[36] have proposed a method of watermarking based upon significant difference of wavelet co-efficient quantization. In this proposed method the work is divided work in 2 categories 1st watermark should be invisible in every aspect 2nd it should prevent some common image attacks like adding noise, scaling, cropping etc. According to the algorithm if the host image is divided according to their wavelet co-efficient and each 7 non overlapping image blocks are considered as one block and difference between two largest blocks are known as significant difference. It has quantized maximum local wavelet co-efficient in a block by comparing significant difference of one block and average significant difference of all blocks by doing this maximum wavelet co-efficient became quantized and value of watermark bits 0 and 1 are showing too much energy difference and this energy is used during the extraction process. In extraction process another function is introduced named as threshold value. On the time of extraction adaptive threshold value and significant difference value is compared and result shows that the algorithm is quite good for jpeg compression and low pass filtering.

Delp J.E. et al [37] have introduced a new and innovative technique of watermarking. To make the watermark more robust against the compression attacks a term named image adaptive watermark is introduced. It means they are designed to resist basic compression algorithm attacks using spread spectrum technique. Image adaptive watermarks are mainly works on transform domain DCT and DWT and main attraction of proposed algorithm is that this transform domain algorithm are already used in image compression and image adaptive watermarking are also worked in transform domain so this method is proposed to match both the algorithm to get a more robust watermarks against compression. YUV color space is considered for their calculation where a 24 bit color image is used and is marked them in color space according to IA DCT they marked luminance plane also and then 2nd copy of original image is watermarked then both the copies are compared and it is found that low data rate matching of compression domain and transform domain watermarking will show more appropriate result.

a different aspect of watermarking is presented in which Destination based watermarks is mainly studied.[38]Destination based watermarks means this kind of watermarks are used in tracking purpose. The attacks which are not able to extract watermark completely but recover few parts of it and the result shows some different figure than the embedded watermarks. They considered additive noise as one kind of attack. And 2nd is how to design an effective watermarking algorithm that can maximize this? Various performance evaluating algorithms and standard process has been discussed. Work is focused around recent advancement of digital image and

video watermarking. Many of them are designed to exploit human perceptual properties among it to provide a high quality performance and intellectual property rights to it. In this work the problem of storing a watermark as serial number in a digital image is discussed another point of authors topic is that a watermark should not be mistaken as another one because 2nd objective of this algorithm is to maximize the number of embedded watermarks. Remarks of this work is algorithm is not been able to pack maximum number of bits from an image but can pack up to number of bits which are useful for practical application. Their modulator bits are low in complexity and only contains the useful bits of an image and it gives the best distinguishing property of a watermarking scheme. It can distinguish up to each and every among 4 billion watermarks.Proposed work describes how watermarking techniques have improvised along with the device criteria and human needs [39].It is shown a very simple watermarking technique to the critical one where they have added that simple watermarking technique can be based on simple common sense and the others are based on basic image processing, modification, lots of algorithm that are more robust and improvised watermarking technique. They have discussed about basic properties of watermarking [3] .few problems like in transparency, robustness and capacity. It is explained that watermarks which are needed during extraction process are called private watermarks and if not needed the watermarking schemes are known as public watermarks. discussion is also made about watermarking standards at first digital versatile disk is introduced for watermark standards but several companies that have denied to use DVD because initially there is an issue in copyright so that later on use of DVD is limited and oriented towards the watermarks detection only. Data hiding sub group (DHSG), Copyright protection technical working group (CPTWG), Digital audio visual council(DAVIC) has proposed so many methods to standardize watermarks in data hiding and copyright protection area. It is described each and every still image watermarking methods in different domains like spatial domain, transform domain, and video watermarking in extension of IA-DCT technique to video, watermarking in MPEG-2, Scene adaptive video watermarking.

Electronic exam papers is one application of watermarking. Due to the requirement of authenticity and protection examination paper needs to be protected using two kind of watermarks one is copyright protected and another is tamper resistant watermark. Whole work is divided in three categories 1st stage they discussed about what are the need of this watermarking methods and solution to it and in other part they focused upon the construction algorithm. Work is presented to design a tamper resistant watermark in two different ways one is to embed abstract information to the title line format, and another is based on attributes of a paper like word, font, characters etc. In last phase of work author applied various active attacks on the watermark and showed that copyright watermarks are more robust and tamper resistant watermarks are able to detect any kind of modification upon exam papers due to active attacks upon the watermark. [40]

A secure data hiding method is presented in which it is shown a resistant against copy attack. A term named hybrid watermarking which are effective for copyright protection, data

authentication and tamper detection. The stirmark benchmarking tool and experimented upon few standard grayscale images are used to show how advertisement and posters can be forged forcefully. Robust part of hybrid watermarking exhibits a high resistivity against geometric distortions. At first description is given about all the necessary points that can be keep in mind while designing a robust watermarking schemes like Host interference cancellation, inter symbol interference cancellation, channel state estimation, geometrical synchronization etc. and after this the encoding and decoding process of robust watermark is described. Another hybrid solution is discussed where it is mentioned that robust watermarks are good for copy right protection where fragile and semi fragile watermarks are better for tamper proofing and authentication so that both are combined to get 3 quality measures at a time and this is the main attraction of this algorithm.[41]

Some basic definition of discrete cosine transform is described in which it is stated that is the most popular and effective algorithm for image watermarking[42]. In this method, the image is divided into a number of different spectral sub blocks. The work is done based on Fourier transform where it converts a signal from spatial domain to frequency domain. Several studies have shown interest in DCT and results in few division basic DCT which can be applied to a signal is known as one dimensional DCT and image always use 2 dimensional DCT because image contains both vertical and horizontal components The Equation of one dimensional DCT is given by

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

For the two dimensional there will be another equation introducing one more component

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

2nd equation is used in image processing where input image is N by M f(i),f(j) is the intensity of pixel in row i and column j F(u,v) is DCT co efficient in row k1 and k2 of DCT matrix. It isexplained that most of the DCT energy lies at low frequency component, 8 bits pixels have 0 to 255 levels. It is mentioned in the paper that F(0,0) represents AC and DC components and though DCT is quite similar with FFT but DCT is excepted worldwide because of its ease in calculation.

This work is purely oriented with 2D DCT discussion in JPEG and MPEG compression. This documentation elaborated the study to another transformation like Hadamard transform, Haar transform, pulse code modulation and entropy and code word assignments.[42]

Vasconcelos N.[43] has proposed an algorithm with some more study on discrete cosine transform (DCT). Here explanation is given for that why DFT is not used everywhere inspite of giving computation accuracy because it has poor energy compaction means it cannot pack much spatial sequence into frequency coefficient, it has quite difficult calculation procedure, it is compared and studied that DCT has much higher energy compaction and higher order spectra than DFT. DCT provides much more concentrated histogram, DCT is giving much better image compression which will be helpful for other applications, DCT calculates only the real components, quantization etc. higher number of bit saving is achieved due to same loss. That's why DCT is preferred over DFT or FFT or any other transform domain algorithm

The term discrete cosine transform is discussed in previous [42], [43] works in details about that algorithm. Cabeen K and Gent P. has discussed the application of the mathematical function. It stated about application of DCT in image processing operation. A detailed study is about JPEG image compression. the whole work is divided in 5 basic step at 1st they split the image in 8X8 blocks then DCT applied to each and every block after that quantization is done on them at 50 % where varying the percentage will give highest compression and poor quality after choosing the best compression level the array of each block will reduce its size so the space consume is reduced drastically after a satisfied reconstruction of the image inverse DCT is applied to the image so the image decompressed after both the matrices of original and decompressed image is compared which shows that the values are slightly decreased without degrading the quality.[44,45]

J. R. Hernández et al. [46] have proposed an algorithm about watermarking for still images using DCT. As similar with [19] it also uses the 8X8 block method for embedding and extracting watermarks.This algorithm is proposed to prevent misuse of watermarks throughout the transmission. Spread spectrum analysis [6] is also used in previous works.. As difference from previous [19] block method author uses PRS generator and a secret key in this method. Main objective of this method is to design a novel algorithm based on DCT domain and which is able to compare new results with theoretical model which can generate the other problems. Author divided his work in few section that are 1.Watermark generation, 2. Watermark verification, 3. Perceptual models are used to ensure the invisibility of the watermark 4. Analyzing DCT domain and embedding watermarks and in last extraction optimal detection is presented. Pseudo random sequence are used to ensure better protection watermark image is not required during the detection and extraction process but DCT Co-efficient of original image is provided for statistical detection process. Author overcomes from common watermarking problems which are resultant of spread spectrum technique like sensibility to geometric transformation rotation, scaling etc. 2D synchronization algorithm and no need of original image is the main advantage of this algorithm. But author couldn't count channel coding scheme for error protection so that they count it as future reference work.[45]

Watermarking approach is discussed using both DCT and DWT[47] . Main objective of the work is to improve quality of watermarking than previous conventional algorithms. For watermark

embedding author took a binary image and scramble it using Arnold-cat mapping then 3 level DWT is applied to the image and DCT of each block is calculated and a PN sequence of watermark bits are embedded to the middle frequency block of DCT. In the time of extraction watermarked image is sharpened using pre filtering method that contains both Gaussian and Laplacian transform to recognize as different from original host image and the embedding process is applied in reverse manner to extract the watermark mid frequency bands and PN sequence relation is been determine to calculate the watermark bits. Result of this algorithm is showing better imperceptibility and robustness than nor DCT or DWT algorithm. This joint process is also good for few additive attacks like noise compression etc.

Su K.J. et al[48] have proposed work based on watermarking scheme is introduced where spread spectrum technique is used for embedding and extraction method author also introduces re indexing of signals means re arranging the samples. Channels of this method are behaving like linier filter this method is limited to additive white Gaussian noise only. Both the detector results are compared accordingly. In 1st part of the work it used some description about abstract communication model then about the watermarking channels. After that direct spread spectrum technique has been described and along with that the embedding procedure, robustness and synchronization, and standard result for additive noise channel is shown. It determines the values in both ways one is to calculate direct sequence spread spectrum co relation factors and another is to calculate the co relation factors after re indexing and then they showed optimal detection and co relation factors for multidimensional cases and compare them all to show that re sampling will give a better resistivity against different noise and will have better synchronization values.

The author has analysed an algorithm using MATLAB and redesign it for Hardware description language[49]. Author uses IMAP and IMAQ image blocks and apply compression to each of them like the watermarking process. Image compression an application of DCT algorithm and this paper is based on that application part only. The error image and difference images are used to reconstruct the image. And difference is calculated using MSE.

Proposed algorithms of this thesis work is oriented with image security features , QR image, watermarking etc. the work is completed with the help of Matlab software. This reference gives a brief description of this software. According to T. Morris ,it is stated that Matlab is used different kind of mathematical analysis, Signal and image processing and graphics related problem this software is designed with the help of basic C language and quite easier to implement than any other Hardware descriptive language. Author also describes from the very basic of image processing operation like how to recognize format of an image how to show the figure in Matlab environment to moderate like to divide it into block and how to implement the harder operation upon it. Author also described level of quantization, use of prewitt, shovel operators and what is histogram and what does it do in image processing. This reference will help a lot the new comers or beginner in image processing programs. [50]

Lu M. Z et al[51] have proposed an algorithm based on multipurpose vector quantization. Traditional watermarking algorithm DCT, DFT, DWT are good for only one purpose so to achieve multiple benefits at a time multipurpose image watermarking algorithm has been introduced. Initially they are based on DFT and DWT but later on they improvised vector quantization but these methods are only good for copyright protection author here proposed a multistage vector quantization method which can be applied on both copyright protection and image authentication. In this method a semi fragile and a robust watermark both are embedded in different stage of VQ (vector quantization) method using different techniques and both the watermarks are extracted without the presence of original watermark. The robust watermark is embedded in the 1st stage of VQ and the semi fragile watermark is embedded in 2nd stage of watermark simple indexing method is used. Author showed that this algorithm is shows better result in copy right protection and authentication and many other aspect.[51]

Zhang Z et al. [52] have presented a work about self-recovery reversible image watermarking system which means the image which are damaged can restore the damaged area as much as possible. Other work focused mainly on the authentication part but objective of this algorithm is to recover the damaged area automatically. To design this algorithm first the original host image is divided into some homogeneous and non-homogeneous blocks by using multiscale de-composition from each block feature information is calculated and considered as recovery watermark. Then host image again divided in 4x4 non over lapping blocks which are further classified as smooth and textured blocks according to the image. The recovery watermark is then generated from homogeneous blocks and error correcting codes are embedded into the smooth blocks by mapping procedure information related to watermark is gathered from the non-homogeneous blocks and error correcting codes are embedded to the non-homogeneous smooth blocks and textured blocks according to the algorithm main objective is to prove that images can recover by themselves if any kind of attacks happen to them the experimental results shows that not only in tamper detection but this algorithm is suitable in high quality embedding because it can hold larger number of information in smaller bit size, and fixed block decomposition is not suitable for tamper detection but multiscale decomposition has given the better result in this point using different algorithms. It is shown that recovery watermarks are generated and compared in different blocks. This algorithm finds a way to recover an image attack with reduced embedding rate.

Khayam S. [54] has proposed a work based on theory of DCT and its application. Exception to the other discussion [43], [44] author here describes properties of DCT algorithm. 1st property is Decorrelation**:** It helps to remove redundancy between neighboring pixels as a result of this uncorrelated transform happened and then it can be encoded separately. 2nd one is Energy compaction**:** It is discussed previously [44] the ability of packing few spatial components in frequency components is known as energy compaction. 3rd one is Separability**:** 2D DCT equation can be divided in row component and column component separately. 4th property is Symmetry**:** the row and column components are also identical in nature or they can be stated that they are

role reversal of each other this property is known as symmetry. Next is Orthogonality**:** The inverse transform of DCT will results in transposed result of DCT matrix. DCT is also helpful in entropy reduction it described a faster DCT equation and compare between DCT, DFT and KLT.

Obukhov A. [55] has presented a work on DCT transform for 8x8 blocks with CUDA. This 8x8 method is used worldwide in case of any kind of image video and audio processing because it shows higher decorrelation rates and it is suitable for all kind of computer platform the main advantage of this block method is that any pair of 8x8 can process independently. Modern CPU based 8x8 DCT are quite costly so author introduced his CUDA based 8x8 image processing to give a technology boost.

Watermarking is the method of embedding secret messages within an image, audio, video or any multimedia messages up to this review we have discussed several methods of image watermarking but in this proposed work discussion is based upon software watermarking. It is designed in a way that P is a program and W is a watermark and these can be embedded and extracted even after P is changed (by changing its code) by translation, obfuscation, optimization etc. W has a mathematical value and it has high data rate and if embedding has done then it will not show any drastic change in P. It is proposed that this method where watermark is stored into the execution steps of the program. In first part of the paper description is given about different kind of attacks like additive attack, subtractive attack, and then static software watermarks, dynamic software watermark is discussed . and then workflow for graphic watermarking is demonstrated and dynamic graph watermarking. watermark stealth is also described which means this kind of watermarks are resistive against all attacks because of some statistical analysis. Main objective of this algorithm is to embed a number into a program which should not degrade the quality of the program and watermark should be extractable even after any kind of transformation given to the main program though it is tougher than normal image watermarking but the goal is achieved successfully.[56]

Li- T. [57] has presenteda work based on 2D bar code which is named as PDF417 bar code it is capable of handling up to one kilobyte of data per label. It has description about some basic properties of PDF417. Each label is 17 module long and contains 4 bar and 4 spaces. Coding principle of this code has follows some basic steps 1. Symbol character 2.Code word 3. Cluster 4. Global label identifier 5. Substitution error. It is a multilayer structure with some blank area the number of contained symbols are equal in both left and right. Author simplifies the encoding technique of PDF417. QR code is the improvised version of this barcodes.

Soon J.T. et al.[58] have proposed a work on Basic structure, properties and application area of QR code . its structure is described in few segments like. Finder pattern: it detects position of QR code , Alignment pattern: It corrects distortion of QR code, Timing pattern: It is used to correct central co-ordinate of each cell,. Quite zone: It is the marginal space that helps QR code to read by sensor and. Data area: As per the name this area holds all encoded data within it. QR

code hold some special features than watermarking like 360^0 high speed reading, resistant to distorted pattern, Kanji and kana characters can also embedded to this. This application is vastly used in various sectors of business like e-ticketing, printing and packaging, hospital, farm etc.

Quick response code or QR code needs to be scanned using a smart device to decode the message into it. The process of recognizing QR code using mobile phones. According to the mentioned work the whole process of detection and decoding involves few steps like at 1st QR code is captured using mobile camera then the QR image gone through grey conversion and after that according to Otsu's method [61] binarization has been done after this filtering means standard opening and closing function is applied to the image to remove noise after that three identical finder pattern is found in three corners of image , author also added that if QR image is partially dirty than timing pattern can be used than finder pattern. In next step alignment patterns has been recognized and with this exact position of QR image is assumed than grid lines are generated and then after some error correction the hidden data is shown to the mobile phone.[59]

How a QR code is generated online is described in presented work using Drupal module a popular 'C' library code to build up a user interface in web browser and encode the QR code.[60]

Zhou J et. al [61] have published a paper upon binarization of QR image in uneven lighting condition which would be helpful for the device to decode the hidden data from the QR image. It is described in detail about thresholding methods i.e Global thresholding and Local thresholding.In global thresholding, only one threshold value is considered for image pixel and back ground but in Otsu's method he maximizes weighted sum of class variance between background and fore ground image pixel's to calculate threshold and shows a good result for histogram of bimodal distribution. In local thresholding**,** multiple thresholding values are selected depending upon image partial environment. 1st one can be divided in various methods like Otsu, KittlerMet, Maximum entropy, Histogram and 2nd one can be divided in Bernsen, Mean, Median MidGray, Niblack .These are known as classical algorithm of binarization which means how well the boundary of an image can be detected. In this paper author compared some definite optimal values of image pixel and some modified image pixel values in uneven lighting condition and showed that they can detect the hidden data more preciously.

Li L.et al [62] have proposed an algorithm which combines QR code with digital watermarking. Additionally this algorithm might be used as security feature of any kind of digital media and resistive against any kind of noise attacks. Conventional DCT algorithm is used for embedding watermark but before some preprocessing steps are done over the QR image like Gaussian preprocessing blur etc. To overcome image distortion watermarks are embedded frequently. Extraction process is completed using fuzzy pattern recognition in absence of original image. This work demonstrated that different noise have different effect on QR image. It is explained that combining both the technology have stronger security influence and to succeed in this pre-processing of QR image is very important. Comparing using intermediate DCT frequency is quite useful step in case of embedding. Remarks can be drawn that it is difficult to forge QR

image when watermarking is applied on them. This technology mentioned proper and quicker response if further research is done .

A new QR code binarization method is presented according to the QR code characteristic to improve the accuracy of QR code decoding in mobile image processing[63]. TheSauvola's thresholding algorithm is modified to solve QR code image binarization which is the threshold decision in the uneven light condition. Experiments show that the proposed algorithm has better correctness of recognition compared with others. Limitation of this algorithm is that it could not hold watermark which is larger than the cover QR image means it could not contain data beyond its capacity and capacity of QR code depends upon its type and type of QR code depends upon the camera performance. According to this algorithm proposed algorithm better for zooming effect but not effective in cropping effect.

To solve the QR code recognition problem caused by ordinary camera collection, the recognition algorithm based on image processing is presented[64].QR code recognition based on image processing fundamentals like Binarization, geometric correction, tilt correction, image normalization done at different illumination condition in different acquisition angle the QR image should be recognized quickly. Experimental result shows that in case of rotation QR image can be extracted and neighboring noise can be reduced efficiently. For other geometric correction Hough transform is not used inspite of this 4^{th} vertex co-ordinate of QR image has been choosen which made the algorithm quicker than before. To reduce the error scaling is used in time of image normalization but it gave an average result. Remark can be drawn that it may be the reference to the future work and which binarization method is suitable for which algorithm should be the 1^{st} priority of any research work because depending upon this the efficiency of watermarks will be determined.

The authgos has concentrated the QR image watermarking method which is implemented at frequency domain[65]. At initial part of the algorithm author described about basic feature of QR codes like . Encodable character set, Symbol size, data characters per symbol,. Selectable error correction in the second part author applied DCT upon the QR image in his prescribed manner and stated that QR code can analyze all input data and identify the characters which to be encoded and it supports extended channel interpretation so it can encode characters and for this it needs error correction and detection model then they convert the input data into bit stream and add indicators if necessary to get a split result they put terminator at the end that they will give 8 bit coded output then divide the coded data into necessary number of blocks to start error correction algorithm, interleave the error correction data and code words of each block and if possible add the remainder bits put them in matrix and apply the masking generate the needed format and version of the image maintaining the dark and light module balance and as a result the watermark is half of the main QR image as if it is divided in two sub blocks. Then the 8x8 block method has been applied on QR image , followed by applying a DCT on each image them P-N sequence is allowed (-1,0,1) as a key .After that information is converted as binary data .Here , watermark is embedded to the mid band frequency than inverse DCT is applied on the

whole image. This describes the whole embedding process for extraction process the inverse DCT is applied on before dividing the QR image in 8x8 blocks previous steps are same. Proposed algorithm uses embedding a text and a key sequence into a QR image to achieve a better security and algorithm shows the results accordingly.

Lin R et al. [66] proposed a new technique named run length coding to encode secret message in QR image. It is cited by the that run length coding means a simple form of data compression technique they used this method to convert the same characters of signal source into repetition character mark. This method is mainly used in where a single data is present for consecutive time like in simple graphics, animated image etc. Basically this run length is used on QR image to the alternate black and white pixels and recombine the data of related run to the adjacent row and column. Before the encoding process some other details like binarization [61] structure of QR image [58] and Process time of QR code it means that how much time the QR code is taken to be scanned is demonstrated. many work r has done on this to increase the speed. presented work focused on shape of QR image and coding process include steps like run length coding, filtering, image seeking etc. and decoding process is the reverse flow of this algorithm. In this work results showed a better quality of error correction, improved pre-processing steps and with a noisy quality of QR image will give a better output. More over main objective of this work is to improve the quality of QR image recognition is achieved.

A Novel secret sharing technique is discussed using QR code[67]. In this work it is presented that any mobile system which has the capture function can scan the data behind the QR image so it will be at risk in case of transmission over any path containing a secret information. For this reason proposed algorithm is designed in a manner that it is helpful in security aspect. using Shamir's secret sharing scheme in this method has divided secret data's in shares of shadows and in the time of decoding if the number of received shadows does not match with threshold value then the message can't be read directly that's why this method is more secure for online and offline transmission and adapted widely.

Presented work is a technique that describes how to embed Arabic characters into a QR code. As it is mentioned earlier that QR image can analyze characters as input data [65] this algorithm is based upon that theory, But main objective of this work is to embed Arabic character into it. It is known that QR image has the capability of embedding kanji and Kana characters [58] so proposed algorithm is designed to embed Arabic characters into it. Using an internal library each word is translated as an equivalent Unicode and space between them is used as break points. It is mentioned that this method is quite simpler than 'Romanization' in that each alphabet is represented by 8 equivalent Unicode.[68]

Sun et al. [69] have proposed an embedding and extracting methods for digital watermarks applied to QR code images. Proposed work is divided in two parts though basic DWT algorithm is used for both of them but in the 1st algorithm objective is to embed random sequence into the QR code and its correlation coefficient is detected and in 2nd method an image is embedded and

extracted using DWT. In case of embedding random serials discrete wavelet transform is applied on original image and among them HL frequency block, a threshold value TI and random sequence of 0 and 1 named as M serial is chosen. When M serial is preserved HL and other blocks are processed with inverse DWT to get the watermarked image. In case of 2nd method a binary image is created and used as watermark in QR image for this there is a size limitation of watermark that its height and width should half of the original HL has chosen and modified according to the DWT parameters. Following steps are same with the previous one but as a difference here 2 dimensional DWT is applied because image is a 2 dimensional array. For the extraction process the steps are again following the same in reverse order they again choose HL band and rename it as HL1 and HL2 and using their equation they obtain N matrix which may reproduce skeleton of watermark image. It included that 1st method is used in higher security levels but 2nd method is applicable on where only basic information are hidden. This algorithm has few limitations like size of the water mark must be half of the original image, image must be a perfect square because QR image itself is a square and the information is embedded to the higher frequency levels of original image that may make it a kind of visible watermark so advanced printing and scanning equipment is needed to make it more reliable.

A blind watermarking technique with some attack detection feature is investigated[70].This implies a key based frame work. It has been designed to embed server address or website address etc. this process mainly used for verification purpose but here it is r compared with communication system where watermarking system problem considered as communication problem embedded data, attack detection as a source encoding, channel encoding and attack detection as detection channel. It is assumed that watermark should attack HH level of source image at 1st level of DWT. Key based approach and attack detection property makes it more robust algorithm in terms of visibility. The finding are similar with the objectives thus it is a good algorithm for watermarking of QR image.

Garateguy et al.[71] have proposed an algorithm based on Optimize image embedding in QR codes. It has mainly focused on the concept of QR images, an automatic method to embed QR codes into color images with bounded probability of detection error. These embeddings are compatible with standard decoding applications and can be applied to any color image with full area coverage. It is the process of embedding color images into QR image but not as hidden message this is opposite of watermarking process that the embedded image is visible and the QR image is hidden. It is compatible with any standard decoding algorithm and applied to any kind of color image with full area coverage. Value of QR image bits are encoded into the luminance values of the color image. To reduce some local distortions they used half toning mask for modified pixel and for luminance level they used non linier programming technique. Some local Binarization techniques are used to decode the QR code. In case of encoding the following steps are taken accordingly half toning, pixel selection, luminance modification, color optimization etc. Discussion is made about various kind of error of this algorithm using a probability error model they introduced probability of detection error, probability of binarization error and global

probability of errors. Experimental results have claimed that the graceful degradation of the decoding rate and the perceptual quality as a function the embedding parameters. A visual comparison between the proposed and existing methods is also demonstrated.

A novel scheme related to authentication techniques is presented using integrity watermarking and QR-Code[72]. In initial stage of the work it is encrypted with a random matrix and it will become an invisible watermark on the cover and it is not dependent upon the content of the paper then the paper is encrypted with QR code and original document is overwritten and not recognizable than previous one and at the time of decryption the original one is needed. It is reported that the mobile phone is an unavoidable device in real time, so authentication of document using integrity watermarking and implementing QR code will be more helpful.

The implementation of Colored QR codes in order to increase data capacity and security yet still maintain reasonably-sized codes is discussed[73]. This work is done to enhance the security and capacity. The main objective of this work is to use colored QR image for capacity and security increment but in presented work some specific sized QR image is used. It uses inbuilt color channel of Matlab to color each QR image in three basic primaries and combine them all so more information is stored in this. It has mainly focused on methods for layering three base colors – Red, Green, and Blue – as well as six base colors – High Red, Low Red, High Green, Low Green, High Blue, and Low Blue. It is stated that the layering colored QR codes effectively have increased the data capacity three-fold and six-fold for three base colors and six base colors, respectively. The layering and un-layering process are fairly simple with the use of some basic MATLAB commands.

The embedding method is developed utilizing the halftoning and error diffusion method[74].A method is proposed for embedding QR image into color image by using half toning technique. This work is presented to achieve a visual satisfaction to the user who are bored of seeing monotonous binary QR images maintaining the robustness in time of decoding. To achieve this at first embedding is done QR image to a color image and that QR image contains the secret data. Basics of QR image is discussed and a QR image is created using Zxing Library. Next as the process of embedding half toning technique is described and it is added that modified pixels are chosen using half toning technique to nullify the effect of blocks and save high frequency details QR image concentrate more data on high frequency regions where human visual system is not working properly. After this pixel selection is another important parameter where it is mentioned that center pixel of QR image is most important for decoding purpose but for various error correction and sampling the adjacent pixels are also needed so a small square block is chosen around the center pixel in-spite of choosing a single pixel and the rest of the portion are used for halftone masking. After that 4 levels of luminance modification is cited and selected pixel's luminance are modified any one of the 4 level that are named as α, β, αc, βc. Then color optimization is done to ascertain some basic rule to select color according to pixel and to choose the best appropriate color a color difference value is calculated in HSL color space. After the whole embedding process the first step of decoding includes binarization calculation of black

and white QR image which is captured using camera and divide into black and white pixel to calculate its threshold values and lastly different luminance value is been calculated. It is explained how to distribute modified pixel based on half tone technique it decrease the visual alteration as a result of whole embedding process. Proposed method are discussed based on structural similarity, tone, color etc. These embedding are designed to be compatible with standard decoding applications and can be applied to any color image with full area coverage. The embedding problem is solved by the integration of halftoning method. Finally, experimental results of the halftoning of color image, embedded QR code image in color image and decoded QR code image from color image are detailed.

Saraswati M.et al. [75] has proposed a work which is focused on QR image watermarking based on DWT and counter let transform for authentication. A new watermarking technique with QR code is demonstrated to protect the secret image. Main objective of this work is to encrypt an image into a random matrix and then it is watermarked (covert*) to the cover QR image. According to the work flow 2 level DWT is applied on the QR image and applied random bit sequence upon the binary watermark image with a secret key. Embedding is done at LH, HL, and HH frequency blocks obtained by 2D DWT. Watermark can be extracted in a recognizable manner. PSNR (Peak signal to noise ratio), NC (normalized co relation), and mean absolute error (MAE) is measured to determine the quality matrices of watermarked and original image and as a future work they stated about quality of watermarked video should be compared with original video by comparing the above mentioned parameters . As the image is first encrypted in random matrix, then it is invisibly watermarked in cover image and no information about the secret image and cover image is needed for extraction of secret image, so it more secure.

Shaikh H. et al.[76] have concentrated a watermarking scheme based on discrete wavelet transform that based on scaling factor. By using the block technology, watermarking signal is embedded into the high frequency band of wavelet transformation domain. The embedding process is described as it divides the main host image into four frequency bands applying 2 dimensional DWT on it. Among the decomposed frequency band the LL1 band can be divided in another four frequency level so author applied Gaussian noise in the image and embed the watermark in the rest of 3 frequency regions (except LL1) in case of extraction the reverse process is followed. By measuring the performance evaluation algorithm author proved that this method of watermarking is not only visually better but it can resist up to Gaussian salt and pepper this kind of noise attacks also but apart from embedding in higher frequency region the main parameter is scaling factor which plays a vital role on visibility of hidden data.The simulation results have suggested that thiswatermarking system not only can keep the image quality well, but also can be robust against many common image processing operations of compression , salt and pepper noise,gaussion noise. This algorithm has strong capability of embedding singal and anti-attack.

Mishra A. et. al [77] has suggested a novel watermarking scheme for images which optimizes the watermarking strength using Harmony Search Algorithm (HSA). The optimized

watermarking scheme is presented based on the discrete wavelet transform (DWT) and singular value decomposition (SVD).The multiple scaling factor is used for embedding. This MSF optimized in harmony search algorithm or HSA is based on DWT or single value decomposition or SVD method. The values which are obtained in LL3 band after modification are dependent upon harmony search algorithm. HSA is nothing but a linier combination of imperceptibility and robustness. The PSNR and SSIM values of watermarked images are good. The amount of modification made in the coefficients of the LL3 sub band of the host image depends on the values obtained by the Harmony Search algorithm. For optimization of scaling factors, HSA uses an objective function which is a linear combination of imperceptibility and robustness. The PSNR and SSIM values show that the visual quality of the signed and attacked images is good. The developed scheme is robust against common image processing operations. It is stated that the embedding and extraction of this algorithm is well optimized, robust and show an improvement over other similar reported method.

Durga A.V. et al [78] has proposed the algorithm for QR image watermarking based on DWT in same manner as presented by Saraswati M.et al. [75] .It shows the embedding in higher frequency domain and extracted also has been done in same manner but as a difference to previous publication author computed and compared only PSNR and NC values and uses binary image as watermark. Presented work is based on wavelet based Algorithm for ownership verification of Digital images It is proposed to show a way of watermarking to give a better copy right protection, owner identification and prevent from unauthorized copying and distribution. Similar discussion about wavelet transform and uses for watermarking has done already but as a new feature a name “filter bank” is introduced. It is observed that DWT is quite simple mathematical operation and applied widely in different fields as an advantage over DFT is that DWT can obtain spatial and frequency both localization in field of signal and image processing, filter banks are perfect tool for reconstruction of any image stated by author it has two channel decomposition and capable of reconstructing structure.

Dawei Z. et al [79] have proposed a chaos-based watermarking algorithm in the wavelet domain for still images A new term chaos based wavelet transform has introduced. The main objective of this work is to redesign the conventional wavelet transform and make it a more robust algorithm against all type of noise and geometric attack. This algorithm is best suited for still image watermarking. The author has introduced a blind image watermarking detection technique with the help of Neyman-Pearson criterion. It is stated that in conventional wavelet transform the whole cover image is divided in few frequency blocks and the watermark is embedded in the higher frequency component but for this proposed work wavelet transform is applied locally means in a sub image (extracted form original image) then watermark is embedded into sub band co-efficient. In the time of extraction original image is not needed as it is a blind watermarking process. The wavelet transform is commonly applied for watermarking, where the whole image is transformed in the frequency domain. In contrast to this conventional approach, the wavelet transform is apllied only locally. Then the subimage has been transformed, which is extracted

from the original image, in the frequency domain by using DWT and then embed the chaotic watermark into part of the subband coefficients. As usual, the watermark is detected by computing the correlation between the watermarked coefficients and the watermarking signal, where the watermarking threshold is selected according to the Neyman–Pearson criterion based on some statistical assumptions. Watermark detection is accomplished without using the original image. Simulation results have demonstrated that high fidelity and high robustness may be achieved , especially under the typical attack of geometric operations.

Sivasankari.S et al. [80] have discussed a new method of adaptive watermarking with higher embedding capacity.The embedding capacity of the approach is controlled through the filter cut-off frequency. The approach is analyzed and shown to have a very high confidentiality due to the sharpness of information recovery with the cut-off frequency. Initially discussion are made about some traditional data hiding methods like cryptography**,** steganography and Digital watermarking.

CHAPTER 3

Security Features

These 3 process is known as basic security feature of Digital and printed Documents

1. **Barcode**
2. **Watermark**
3. **QR Code**

3.1 Bar Code: [83]It is a machine readable code, a strip of horizontal black and white bar with variable width and same height. It hold a series of number and letters and printed upon a package to trace it in time of parcel, in time of stock management it can help to check the stock (it carries the batch code), It can give brief idea about the package before unboxing. Earlier barcodes are designed in a way that it can carry data in one direction thus it is 1D barcode and codes are holding only bars but later on 2D barcodes are designed and as symbols rectangle and hexagons are used.

Fig 6: Structure of a Barcode

Advantage of Barcodes:

- **i.** It hold only one directional data which are easy to generate and decode so barcodes are time saving.
- **ii.** Normal optical reader can decode it so it is quite economic no special hard ware or software are needed.
  To trace or locate a package or to check the stock barcode is quite good solution.

Limitation of Barcodes:

- **i.** It always need an optical reader to read the code
- **ii.** Any kind of tampering or piercing will lead to failure of reading the code.
- **iii.** It can hold a smaller amount of data in one direction for large amount of data barcode is not suitable or 2D barcodes are used.

3.2 Watermark: It is the process of imposing copyright to some data both in digital and physical mean. Watermarks can be visible or not visible. Visible watermarks are used only for imposing or showing some ownership proof but digital watermarks are the invisible one and used to hide data to impose ownership or copyright protection. Physical watermarks can be designed through dandy roll or cylinder mold process and varies in terms of shades (light,dark or transparent). Digital ones are embedded through some mathematical algorithms using some software and cannot be extracted in between. Imposing watermark with in an image, audio or video files are popular process among researcher and widely used in security system of digital or physical media transfer.

Fig 7: Example of overt watermark. Fig 8: Example of covert watermark

- **Basic properties of Watermarks:**

a. Robustness: It is the property of a watermark to check how strong it is or how it can prevent the various kind of geometric distortion and attacks.

b. Imperceptibility: Watermark is imperceptible means it is not visualized by human eyes nor audible to human ears normally, so a good watermark means it should be imperceptible and only can be extracted by some special processing only.

c. Secure and Reliable: Watermarking is the secure and reliable place for data hiding it uses some special kind of marking signs that cannot extracted by everyone.

d. Low Complexity: The algorithms are used to embed extract and detect the watermark from the original signal are less complex that made the watermarks more useful and effective.

e. Secure hiding Place: Watermarks are carried or hidden in the component of the carrier signal so that it can prevent the watermark to prevent any kind of destruction or any kind of format change.

- **Advantage of Digital watermarking:**

a. **Copyright Protection:** Copyright means the original authority to protect, redesign or modify any data it can be of any kind of data like text documents, images, audio etc. Watermarking is a process to impose that protection to the data so that any kind of unwanted modification can be prevented.
b. **Data Authentication:** Watermarking can be used for data authentication means it can track the origin of the data that from where it is actually been sent. Some specific Watermark is imposed to the data at the time of origin so that the receiver can easily trace from where the message come from.
c. **Broadcast Monitoring:** Some specific broadcaster have their particular time of broad casting their show. To prevent overlapping broadcast monitoring is needed which happens with the help of watermark.

d. **Owner Identification:** From watermark the original owner of some data can be recognized.
e. **Tamper resistance:** There are several types of attacks can be applied to a watermark some of them are called Active attacks in this kind of attack the attacker wants to recover the secret message properly and another one is passive attack in this type of attacks attacker don't need the secret message but want to destroy the data so that the watermarking algorithm should be designed in a manner that it could be tamper resistant.

- **Limitation of watermark:**

i. Overt watermarks are easier to design and copy

ii. Covert watermarks are much safer than overt ones but they need sound knowledge of most effective algorithm to embed data and secure them from external attacks.

iii. Decoding also need exact knowledge of algorithms which are not possible for common people to decode and read the message.

- **Types of Digital Watermarking:** Digital watermarking can be classified in many categories

a. Working domain (spatial domain, transform domain)
b. Document type (Text, Image, Audio, video)
c. Human perceptivity (Visible, Invisible)
d. Availability of reference image (Blind, Non Blind, semi blind)
e. Based upon working domain watermark can be categorize as
f. Based upon human perceptivity watermarking can be divided two categories they are described below

- **Covert Watermarks:** Covert means the invisible watermarks which can't seen by naked eyed or some time it is not present in the digital file but when we print it can be visible in the printed copy.
- **Overt Watermarks:** Overt watermarks are the simple or general watermarks which are visible these are created by the dandy roll process or cylinder mold process.

g. Based upon reference image availability watermark can be divided in two categories

- **Blind Watermarking:** In this technique the original reference image is not needed for the extraction process.
- **Non Blind Watermarking:**In this process the Original reference Image is needed in the extraction process.
- **Semi-Blind watermarking:**Not completely but a little amount of information about the reference is needed during the extraction process.

Steps of Watermarking:

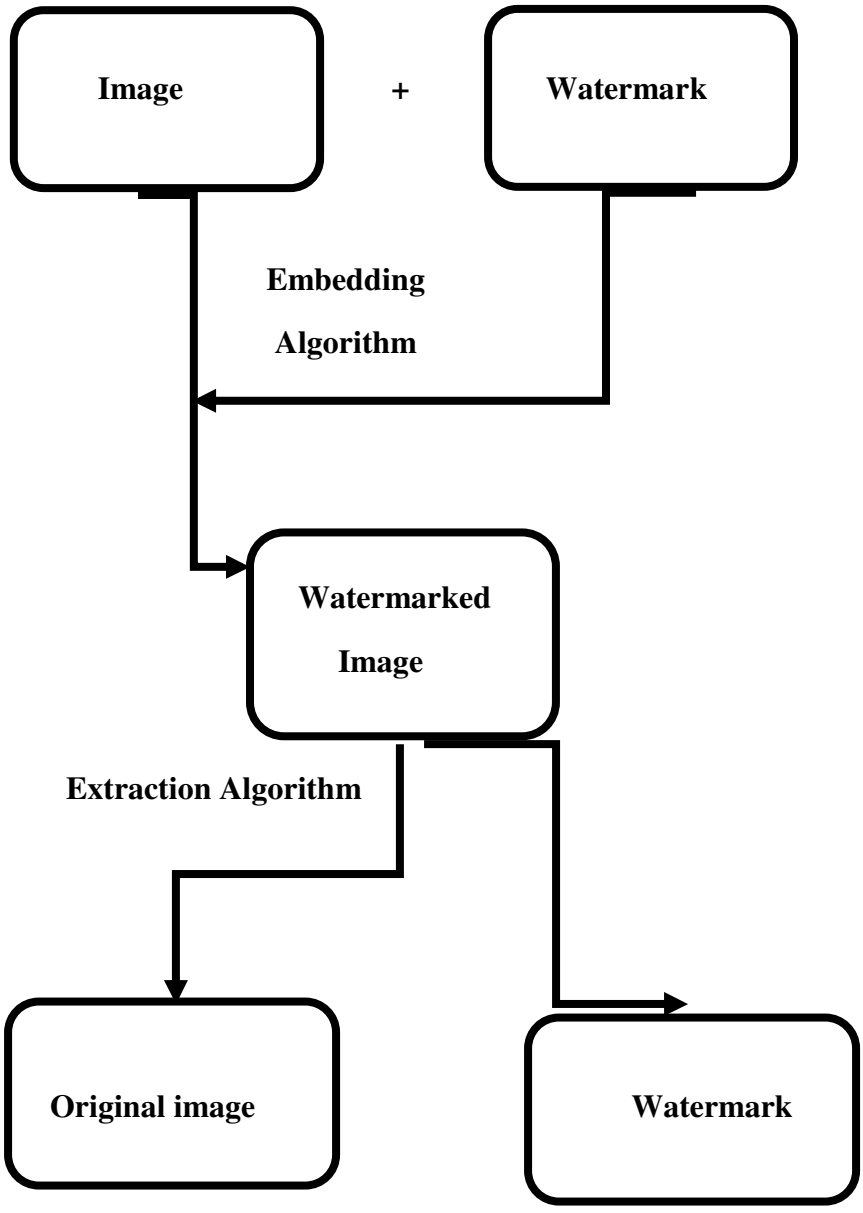


Fig 9: process of image watermarking

3.3 QR Image: After the Barcodes in 1994 Denso wave Company which is one of the major Toyota group of company invented QR image or QR code. This QR code received approval as an ISO international Standard in 2000. This QR images have their specific structure and can be used by everyone because Denso Wave released their patent in public domain. It is a perfect squared shaped structure with small black and white shaped dots and box containing in it. Initially QR codes are only black and white in structure but now a days QR images can be customized as per owner's choice (variety of colors, using logos). The color QR code doesn't affectthe scan-ability of the image. One precaution to be taken that code should be designed in dark color and placed against a light colored background. Inverted QR codes are also acceptable.

Fig 10: Conventional QR Image

Fig 11:One color QR image

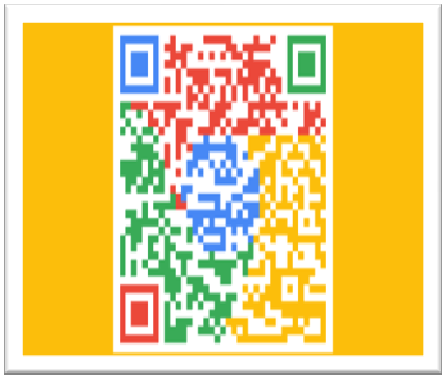


Fig 12: Multicolor QR imag

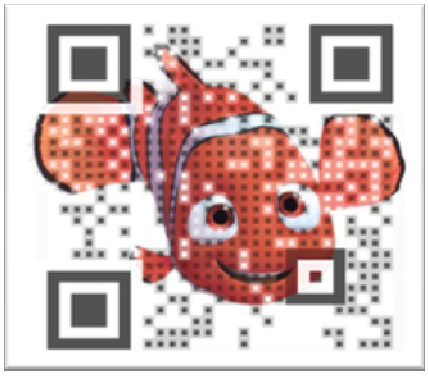


Fig 13: QR image with optimized logo

i) Structure of a QR Image: As we discussed QR code is a square shaped structure and inside this there are specific small cell shaped structure. The whole structureis similar as matrix structure. QR images are have some basic common feature like Finder pattern, Alignment pattern, Quite zone and data area etc.

Fig 14: Internal Structure of a QR image

a. **Finder Pattern:** It is placed in three corners of the QR image and helps to detect the size, position and angle of QR code. This pattern can read or detect in all direction (360^{o}).
b. **Alignment Pattern:**This pattern is placed in a QR code to correct the distortion rather we can say it is best fitted where the distortion is non-linear. Central co-ordinate of this alignment pattern is used to correct the distortion. A black isolated cell is placed in this it helps to detect the central co-ordinates of this pattern.
c. **Timing Pattern:**Timing patterns placed in a QR image in both vertical and horizontal manner. It is used for identifying central co-ordinates of each cell and designed in an alternative manner of arranging black and white cells. It can correct the distortion of each and every data cell when the central co –ordinates are disturbed it can also recognize that when or where the error has occurred.
d. **Quite Zone:** The four particular cells are dedicated as the quite zone. Main work of this zone is to separate the QR image from any other image that can be read by CCD sensors. As for good reading and detection some margin space are needed the quite zone is doing that work with an efficient ease.
e. **Data area:** This area is the main working zone of a QR code, here the encoded data are stored and hidden from bare eyes. The encoded data's are inserted into this code by obeying some particular encoding rules. The data which to be encoded is first converted to the equivalent binary number and then they are converted to specific black & white cells arranged according to the data. In this data area a special feature

is incorporated which is known as Reed-Solomon and is used for error correcting operation.

ii) Charactertstics of QR Image: Characteristics means the special features by which it will be decided why QR image is preffered over Barcode and other two dimensional security aspects. That special features of a QR image is described below.

a.360^{o} high speedreading: As previously discussed that QR codes are having finder patterns they are cepable of finding angle position and size of the QR code and this pattern will provide all direction reading flexibility.Finder patterns are placed in 3 cornres of the QR image and black and white cell ratio is 1:1:3:1:1 and will visible from any direction (360^{o}). other 2D barcodes are taking time and proper angle should be detected properly to retrive the information but for QR image the process is quite faster because CCD sensor 1st captures the reading matrix symbol and then store it in a memory.

b. Data restoration function: This feature allows a QR image to recover its data when it is smudged and damaged. This error correction property has 4 level upto which it can retrive data properly the levels are 7%, 15% ,25% and 30% according to the area of the QR image. Reed solomon codes are also helpful in this purpose of brust errors this codes are placed in the QR data area and when this kind of error occurs. If there is a possiblity of smudging or damaging the QR image then it should be set to 30 % error correction level in the time of designing the QR image.

c. Resistance against distortion:A QR image may be distorted when it is **s**et to a rough surface or if the reader is tilted than it became difficuilt to scan the code. To overcome this problem QR codes are having allignment patterns which are placed with in a QR image in reguler interval. The variation between the centre position of the allignment patterns are create great mapping and made easier reading for linier non linier distorted QR Images.

d. Linking feature:A normal QR images are having liniking functionality this means a normal QR image can be divided into several separate QR images. A single symbol can be divided up to 16 symbols as maximum. By linking QR images in any order reader can be able to read the QR image this feature is good for printing of QR images. It is suited best where the space is not so wide to print the whole Qr image than any part of the image can be printed and data can be linked after.

e. Masking feature: It is known that QR images are arranged the black and white cells in a balanced way. It has special patterns for masking process to acitivate this masking feature some EX-OR calculations are took place between the data area cell and the masked pattern cell which are also known as template cell. There are eight mask patterns and each of them are evaluated and the mask pattern which have highest result are stored in the data area.

f. Confidentiality of the code:QR codes are more confidential than other security feature because the relationship is made between the character type and stored data type which are

designed for the special uses only so it can be encrypted easily but in case of decryption if the convertion table between both the character type and stored data types are not ciphered then it will not possible to read by anyone else.

g. direct marking process:QR images are able to embedd some data directly means the data which are marked directly using laser or dot pin markers. QR images can give readability to this kind of data also. Directly marked QR images are not all time have their same square shape they can be of circuler shape or the black and white part can be inverted. But inspite of all this QR images are readable and can read from the back side if placed in a glass top surface.

h. Kanji& Kana character support:QR images are 1st designed at Japan for their own use so it will have some in built support of having the readability for kanji and kana characters (alphabates of Japan). QR codes can embedd japanees characters 20 % more efficiently and also support chinees chacrters set.

3.4 Limitation of QR code:

- QR codes are widely used in China but it has less uses India because of public unawareness.
- It is not useful if a consumer does not have any mobile device like smart phones
- Exact knowledge is required to decode and encode QR codes.

3.5 Application of QR code:

1. It is used to hold product information like manufacturing date, expiry date, shelf life etc.

2. It is used for money transfer

3. In store and hospitals to check availability of blood, medicine etc.

4. Helps us to monitor our social networking account to on different devices.

5. China and Japan adapted QR code so widely in their industries they used them in restaurant to farm, form air to railway ticketing system etc.

Chapter 4

Attacks on Watermarking

There are so many types of attacks that can be applied on the digital images few of them are discussed below. Red arrows are signifying the attacks which is used in proposed algorithms have use for our work.

Cropping
Flip
Rotation ⟵
Scaling
Line removal
Color Reduction
Sharpening
filtering
Noise ⟵

i. Cropping: Cropping is nothing but cutting a part of an image from any direction. It can be necessary for some cases like extremely enlarged image or where we want to remove unwanted outer area but it is considered as an attack if it is applied to some data which carries some secret information within it. For Watermarking method image cropping is destroying the secret data in most of the cases.

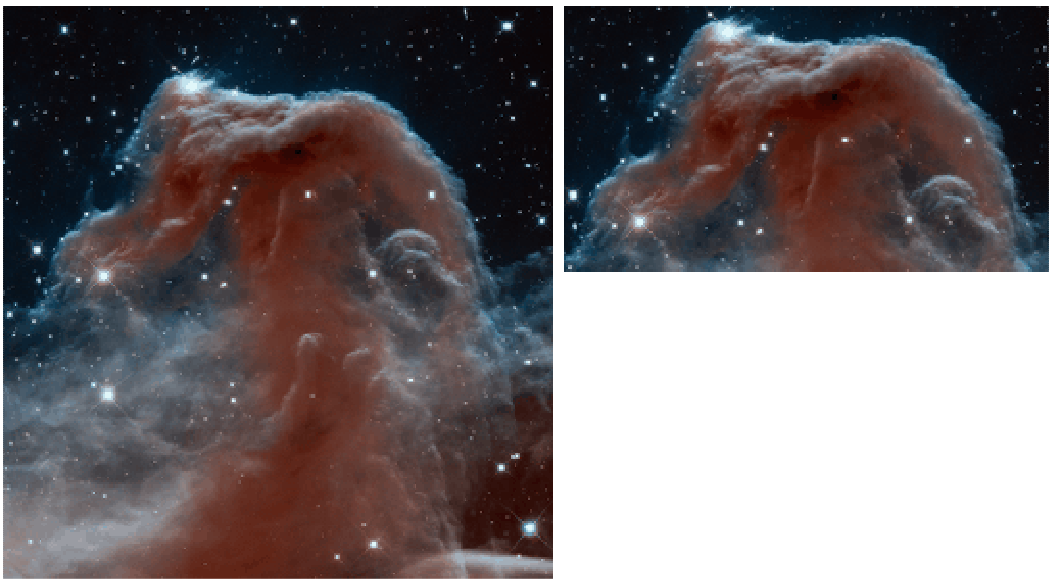


Fig15: Cropping of an image

ii. Flip: A flipped image is an image which produce mirror effects of movable objects it can be also named as reverse image. It is mirrored across the horizontal axis.

Fig 16: Flipped image

iii. Rotation: It is a feature that allows an image to move clockwise and anticlockwise direction. For image processing rotation can be applied by mentioning the angle values like 35^0, 45^0. We will observe the effects of rotation in our work and see which algorithm is best suited for this type of attacks.

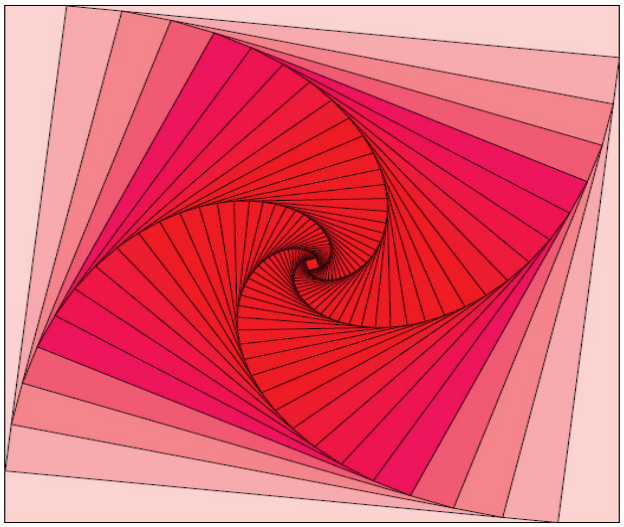


Fig17: Rotated image

iv. Scaling: It means to rescale an existing image by applying this feature we can make a bigger or can make a smaller image without cropping or editing the image excess use of scaling may results in a loss of details from the images means it can cause a quality degradation to an image if not used in limit. It can harm a watermarked image because extreme big or extreme small images are not able to hold all information properly.

v. Line removal: Hence this kind of attacks are rare but it can remove a vertical or horizontal line or can remove too many lines from theimage at a time. This kind of attacks can also challenge watermarked image or hamper the privacy of the document.

vi. Sharpening: It means to enhance details of an image towards the edges of the image it can modify the details in an image excessive use of image sharpening can reveal the data in the edges and this kind of attacks are may be harmful for image watermarking.

Fig18: Image sharpening

vii. Filtering: Image filtering means using different kind of filters like high pass, low pass etc. to give various effects to the resultant image. It can changes the shades of color, number of pixel in some particular rule. Filtering can be done by using the image filters which can pass through or prevent some kind of signal.

Fig19: Image using different filter

viii. Noise: in general it can be said that noise are the disturbance present in the channel during the transmission of any kind of signal. Noise can be different kinds in case of image noise can be present their due to some problem or disturbance in the image sensor. It can degrade the perceptive quality of an image drastically. We have applied this attacks in our both algorithms and observed the results.

There are so many kinds of noise like Gaussian noise, Salt and pepper noise, Shot Noise, quantization, film grain, anisotropic, periodic noise but for our work we are only discussing the 1st two noises only.

Gaussian Noise: Image sensor can cause this kind of noise which is arise due to image acquisition and the sensor inherits some noise because of illumination and own temperature. Gaussian noise are pixel independent and additive in nature.

Fig20: Image with Gaussian Noise

Salt and pepper Noise: It is also known as spike noise or impulsive noise. Salt and pepper noise are spread in an image in a manner that the dark noise pixel are placed in the lighter place of the image and light noise pixel are placed in the darker zone.

Fig21: Image with salt and pepper noise

CHAPTER 5

Basic Watermarking Algorithm

The process of watermarking use many algorithm we can categorize them 3 parts

1. **Embedding Algorithms**
2. **Detection Algorithms**
3. **Extraction Algorithms**

   The above mentioned 3 categories are implies when the algorithms can be applied but it can be divided as per working domain they can be of

   1. **Spatial domain algorithms**
   2. **Transform domain algorithms**
   3. **Spread spectrum algorithm**
   4. **Performance Evaluation algorithms**

5.1 Spatial Domain Algorithm: In these technique the watermarking is inserted directly on the pixel that's why it is a quite easier process than any other techniques.

a) **LSB Algorithm:** In this domain watermarking uses the least significant bits of an eight bit image which does not effect perception of human visual system watermark is hidden into the least significant bit of the image. It's the simplest algorithm among all.

5.2. Transform Domain Algorithm: In this technique the watermark is not added with the intensity of an image, it is added with the values of transform coefficients. It took the normal HVS characteristics to its account while transforming the image in frequency domains. Transform domain algorithm can be categorized in three:

a. DFT (Discrete Fourier Transform): Discrete Fourier transform is an algorithm in which images are divided in different sine and cosine components. The inputs are in spatial domain but the resultant images are in frequency domain. In this algorithm each point defines particular frequency that are present in spatial domain. It is used in various fields like in reconstruction of image, filtering etc. DFT contains complex part in the calculation so that it is more accurate but it is more complex in calculation and hence time consuming so that it is not widely used in image watermarking.

b. DWT (Discrete Wavelet Transform): Wavelet transform is a technique which can split the lower frequency signals into another higher and lower sub parts and again the lower one to the next sub parts. It mainly applied on the edge of an image which contains the higher frequency signals. It is a time domain analyzed localized method and having fixed window size. It changes a discrete time signal to a discrete wavelet transform the divided basis functions are known as wavelets.

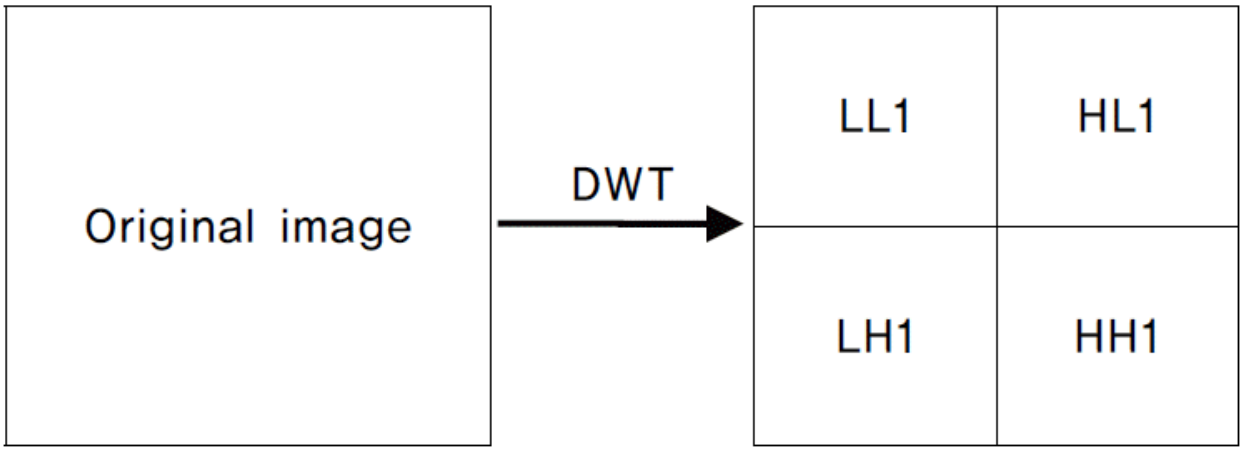


Fig 22: Decomposition of an image using DWT algorithm

c. DCT (Discrete Cosine Transform): Discrete cosine transform is a technique which is a kind similar to DWT but the only difference is that it can broke up the image in several frequency bands and embed watermark into the middle frequency bands which is quite easier process and its chosen in a manner such that it does not contains major visual important parts (e.g. wide region of similar color).

The reason of Choosing DCT over DWT and DFT??

1. We can obtain a much more concentrated histogram in DCT for a particular image than DWT.
2. DCT can wipe out the nonessential parts of an image without any extra loss of bits.
3. It will give more energy compaction than DWT.
4. It can save bits in same kind off loss.
5. DFT calculation is quite complicated so it is not used by everyone
6. DFT will give discontinuities while DCT will show symmetry because of y (n) if we try to eliminate this discontinuities the image will loss lots of high frequency areas from the image that's why DCT has been choosen over this two algorithm.

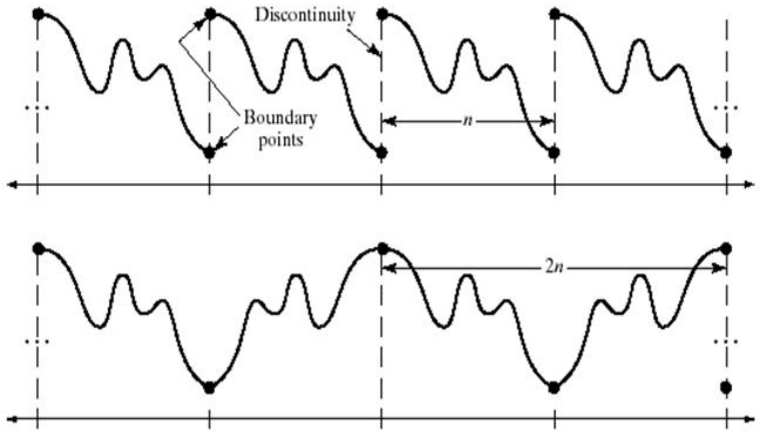


Fig 23: Comparison between Discrete cosine transform to Discrete wavelet transform

This is the equation for 2 dimensional DCT

$$b_{k1,\,k2} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-2} 4a_{(i,\,j)} \cos\left[\pi_{k1}/2_{N1}\,(2i+1)\right].\ \mathrm{Cos}\left[\pi_{k2}/2_{N2}\right](2j+1)]$$

Where a is the input image b is the output image height of the image is N2 and width of the image is N1 a ($_{Imp}$) is the intensity of the input image pixel in row i column j and b(k1,k2) is the DCT co efficient of the DCT matrix in k1 row and k2 column.

Image can broke up the 2D DCT in one dimensional DCT and use that in both horizontal and vertical manner or rather we can say in a row wise and column wise.

There are two ways we can find to compute DCT firstly using the FFT based algorithm to embed the image and it will give a speedy computation for large inputs.

The second method is to use the discrete cosine transform matrix which is more useful for small square matrix.

This can be applied to each and every column of the matrix. The equation is as follows:

$$T_{pq} = 1/\sqrt{M} \qquad \textbf{when P=0, 0≤q≤M-1}$$

$$= \frac{(\sqrt{2}/M)\cos\pi(2q+1)p}{2M} \qquad \textbf{when 1≤p≤M-1, 0≤q≤M-1}$$

For MxM matrix A, DCT value of the column of A is T*A and 2D DCT can be computed as B=T*A*T' and the reverse can be computed using B=T'*A*T.

****Watermark co-Efficient:** This can be known as embedding co efficient of watermark a scaling factor (here it is α) is used to recognize the strength area where the water mark should be embedded .This co efficient can affect the visibility of the watermark through the host image. It can be applied to the image with the knowledge of masking phenomena this equation can be used:

$$V'_i = V_i(1+\alpha X_i)$$

Advantages of DCT Algorithm:

It can prevent various kind of attacks like Noising, filtering, compression etc.
It is applied on the middle frequency zones pseudo random sequences are which can help to embed the watermark more easily and does not effect HVS characteristics because human eyes are not very sensitive to that much minute changes.
It uses the .Jpeg compression methods to apply watermarking which make the mark more robust in nature.

Performance Evaluation Algorithms: There are various kind of algorithm which are attached with watermark embedding and watermark extracting process many of them has been discussed already but except all this there are some more algorithms which are employs with the performance evaluation of a watermarked image. It is a very important part of any watermarking process it shows how effective a watermark is. It mainly evaluates the quality matrix of an algorithm. The algorithms are as follows:

1. MSE (Mean squared error) Algorithm: the main objective of this method is to evaluate the no of average square error between the host and resultant image or watermarked image.

$$\text{MSE}=1/\text{MN}\sum_i M \sum_j N \, (Wij - Hij)^2$$

Here M, N are pixel value of host image, Wij is the pixel vale of watermarked image and Hij is the pixel vale of host image.

2. PSNR (Peak signal to noise ratio): We know that noise can degrade the quality of any image so this algorithm is used to measure the efficiency of the watermark with respect to noise or rather we can say that by this algorithm measured that whether the watermark is imperceptible (noticeable with naked human eyes) or not.so the equation is as follows:

$$PSNR = 10 * \log P^2/MSE$$

Here p is the maximum value in host image.

Chapter 6

Methodology

In this thesis work the comparison between two process of coding is described both the process uses DCT algorithm but in two different ways. These Experimental methods can be can segmented out this work as 1st and 2nd process of Image and QR image watermarking and after that a comparative study has been done between the result in effect of various attacks and distortions.

Flowchart of Proposed Work is illustrated in Figure 24.

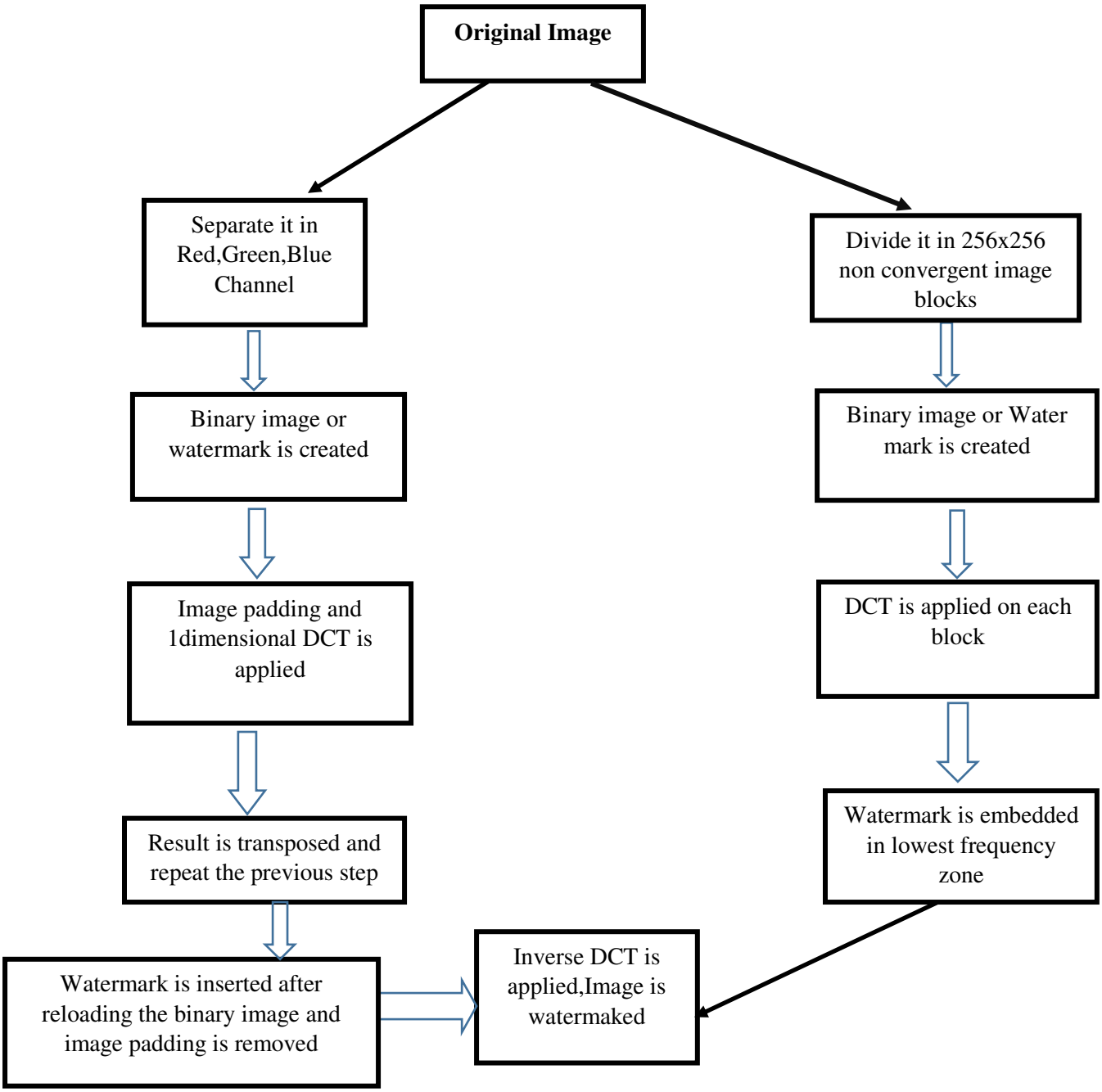


Fig 24: Flowchart of proposed work

Channel separation Method: This can be named as DCT Channel separation watermarking the steps involved in the Algorithm are given below

Embedding Algorithm:

1. One color image in this case a baboon image from Google image is chosen which a rough image with so many color variation is. It will be treated as the Cover image or the main host image.
2. Generate a binary image using Matlab this will be the watermark.
3. Save the data of the binary image into an 'm' data file.
4. Separate the cover image in corresponding R,G,and B channel.
5. Apply image padding in to each channel to the number of two in both direction
6. Apply one dimensional DCT in individual channels(padded image channels)
7. Transpose the result of step 6 individually
8. Then DCT is again applied on to the 3 channels
9. Again transpose the result of step 8
10. Reload the saved m.dat file (saved data of binary image)
11. Introduce a watermark strength co-efficient which on which visibility of watermark will be relay.
12. Take a matrix of size mXm whose row and column rm and cm respectively.
13. Multiply the data of the m file with the watermark strength co-efficient and equate it with the previous row column of I1, I2, and I3.
14. Apply the idct2 in a same manner like DCT in both the dimensions (vertical and horizontal).
15. Remove the padding from each channel.
16. Recombine and store the resultant channel data to a variable named 'y'.
17. Show the embedded figure in the output.

Block Division: DCT Block division method. In this section a color image is taken1st and divide them in several blocks that's it is called Block method. In this case also we compare the algorithm in both the color image and QR image steps are as follows:

- An image of length 256X256 is taken and generate a binary image of size 32X32
- Read both the image in array of I and J took a constant K=8
- Split host image into non convergent image blocks value limits up-to $1 \leq x,y \leq 8$
- DCT is applied to each block of the cover image

After that element of watermark image is applied to the lower frequency zone of the cover image for our image it started from block (1,1)

- Both the image are combined using watermark embedding strength equation by Cox et al.
- Inverse DCT is applied to the embedded watermark and combine the image in cover image I
- Extraction process of the watermark is just the reverse of embedding order as a difference we have done a judgement of strength co-efficient α by making watermark $w(p,q)=0$ when $\alpha<0$ and 1 when $\alpha>$ o and value of p,q is $1 \leq w(p,q) \leq 32$;

Chapter 7

Results & Discussion

Two watermarking Algorithms will be compared in this section. In both the methods algorithm is applied on Normal color image and after that on QR image. Following images shows the results of the experiment.

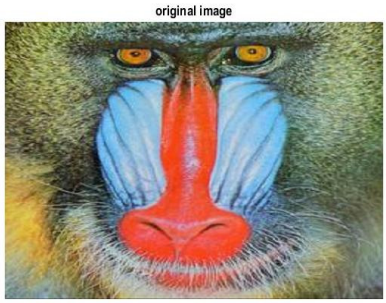


Fig25: Original host image of channel method

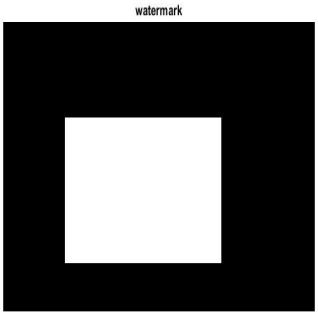


Fig26: Binary watermark image

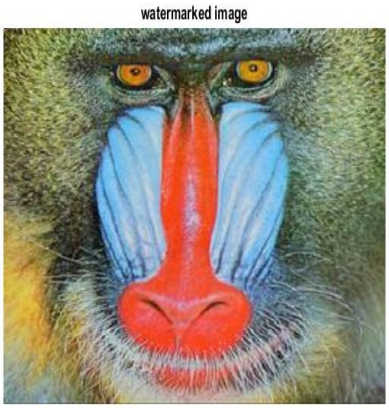
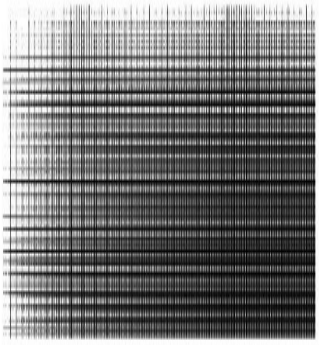


Fig 27: Watermarked image



F28: Difference between original and watermarked image

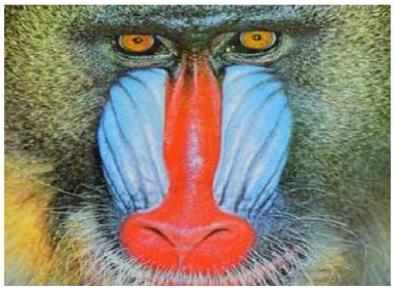


Fig 29: De watermarked Image

Fig 30: Difference between de-watermarked and original image

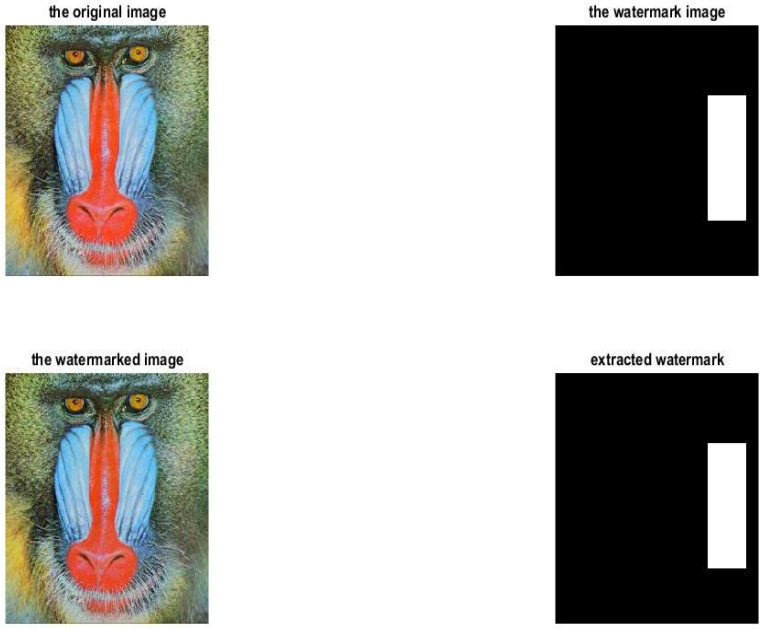


Fig 31: The embedding and extraction process using DCT Block division method

Figure 24 shows original Baboon image which is treated as host or cover image, figure 25 shows binary watermark image. The watermark is embedded using the channel separation model and result shown in Fig 26 (watermarked image). In figure 27 difference between original image and watermarked image is shown. Figure 28 and 29 depicted Watermarked image after extraction and difference between Extracted cover image and original host image. Fig 30 represent embedding and extraction both using DCT Block division method. It is observed from the above figure that in both cases watermarked image is perceptually same as the original host image. In case of extraction, channel separation method cannot extract the watermark after embedding, So that a difference image is represented in fig 27. It reflects the difference between Original host image and watermarked image. It shows the amount of change that the original image is faced after the embedding. As the watermark image is not properly extracted so after De-watermarking the difference between original image and extracted cover image which is shown in fig 29. It shows a complete black image which means there is no difference between the original and de-watermarked image. So it can be added that the watermark is extracted completely.

For DCT block division method embedding and extraction is shown in fig 30 It shows a good embedding of watermark and a better extraction also. Both the Watermark and cover image is combined and extracted properly.

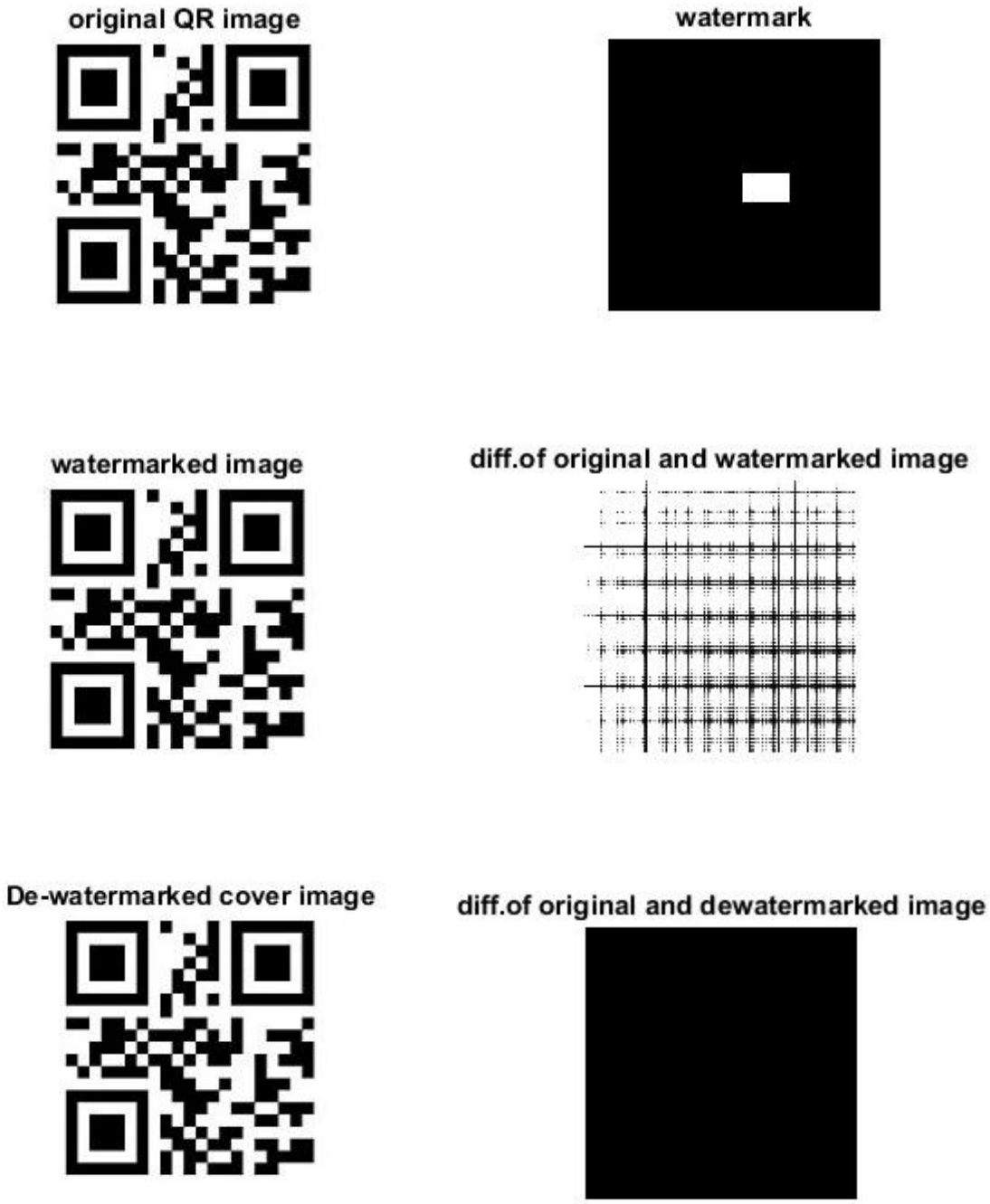


Fig 32: QR image watermarking using DCT channel separation method

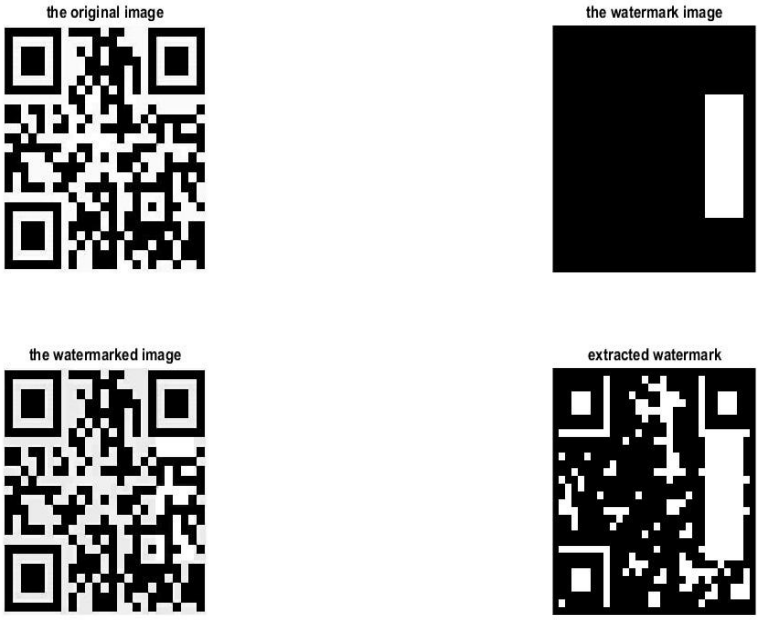


Fig 33: QR image watermarking using Block Division method

Same two algorithms are applied in QR image and the results are depicted in Fig 31 and 32. Like the normal image watermarking using channel separation method the results of QR image watermarking is same. It shows a good watermarked image and fully extracted cover image which has no difference with the image before embedding. In the block division process the result slightly varies from the normal image watermarking. It is not showing a good quality embedding and the watermark is not recovered properly as it shows before in figure 30.

Another aspects of comparing these two methods are described next.

Calculation based on image matrix: For the Channel separation of embedding the image matrix of input images are as follows: table shows the value through 7x5 columns'

114	105	77	70	93	89	62
149	122	85	73	92	99	85
122	114	107	95	84	77	72
90	100	116	114	95	79	71
53	76	109	125	121	106	88

Table 1: Matrix value of input image for Channel separation method

287.6144	10.9048	-24.5068	76.6878	66.9690	83.3415	102.1795
-59.5636	235.0369	206.9405	64.9659	123.2711	105.7975	36.7322
100.8550	125.4601	119.3628	94.1855	87.1704	77.6892	67.1064
128.2580	79.2650	93.6317	115.4737	89.2638	77.7531	79.8541
64.1951	69.9325	102.4546	125.4312	119.3215	105.6351	90.5909

Table 2: Matrix value of output image for Channel separation method

Table 1 shows the input image for Channel separation method of original cover image and Table 2 shows the output image for Channel separation method of water marked image.

106	73	97	56	85	113	131
146	72	101	89	76	64	66
105	110	81	68	83	104	99
60	127	116	85	92	115	88
46	87	136	88	86	161	106

Table 3: Matrix value of input image for block division method

100	67	91	50	79	107	125
140	66	95	83	70	58	60
99	104	75	62	77	98	93
54	121	110	79	86	109	82
40	81	130	82	80	155	100

Table 4: Matrix value of output image for block division method

Table 3 shows the input image for block division method of original cover image matrix values and table 4 shows the output image for block division method for watermarked image matrix values. As observed from the data table 1,2 and 3,4 that in both the method showing a huge difference between input and output value. Tables 1 and 2 are showing input and output data comparison of channel separation method, the results shows that they are considering values up-to 4^{th} decibel place and as well consider the negative values which defines that this process is resulting in a more accurate output.In the table 3 and 4 data are simple and easier in calculation hence it will take lesser time to run and find a better result.A noticeable difference is that the value of output image in block division method is lower than the input image, which means this method is creating compressed result. Whereas channel separation method is creating a higher quality output image.

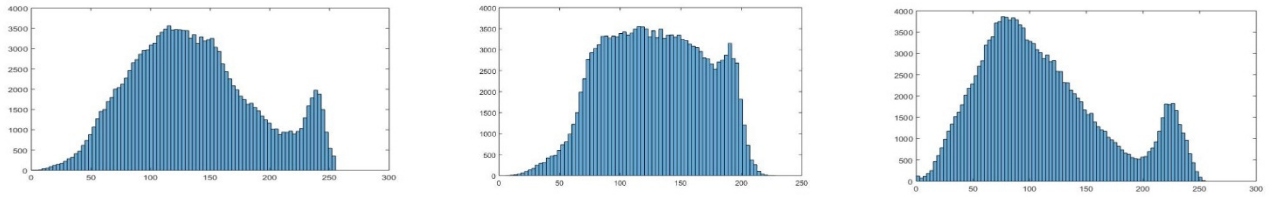


Fig 34: Histogram of Baboon image (for all input channels using Channel separation

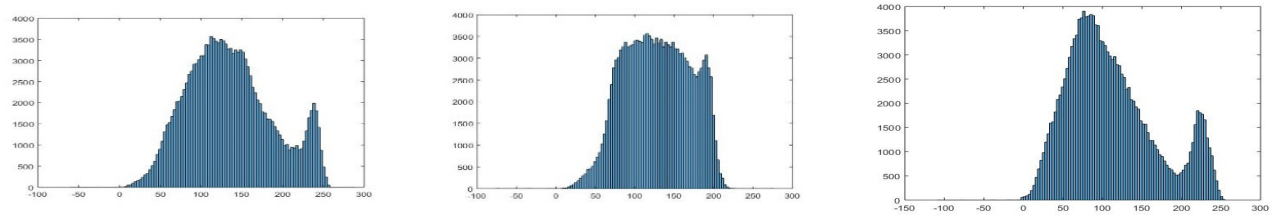


Fig 35: Histogram of Baboon image (for all input channels using Channel separation method

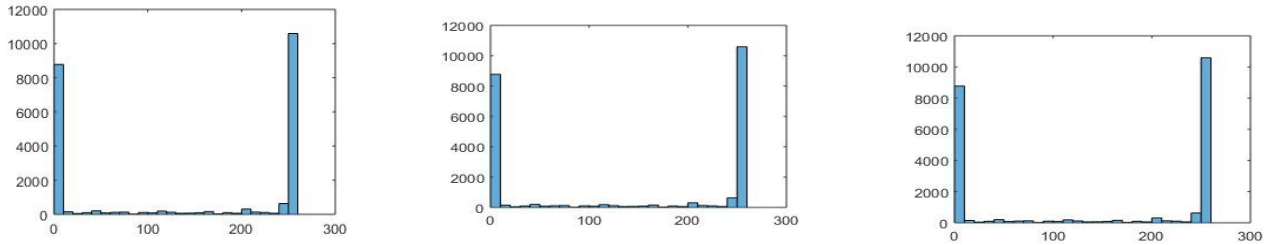


Fig 36: Histogram of QR image (for all input channels using channel separation)

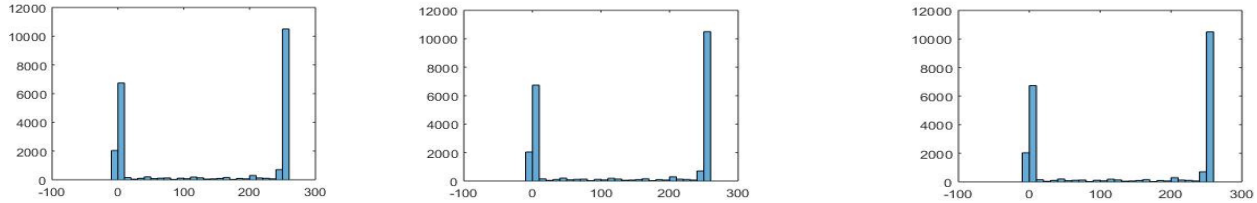


Fig 37: Histogram of QR image (for all output channels using channel separation)

Discussion based on histogram of Channel separation technique: Figure 31-32 shows histogram of each channel of Input Baboon Image and watermarked Baboon image. Some remarks can be taken from the images that are-

i) All the histogram of each channel is shifted towards right. As we know that shifting the bins of histogram towards right means that the shifted histogram will construct a better and brighter image. In this case if we compare both the images the watermarked image is quite brighter and prominent than the original image.

ii) For both input and output image, channel 2 means the green channel is giving the best result because it shows more numbers of peaks. It means that intensity of pixel are higher on that area.

Figure 33-34 shows histogram of input and output QR images and it shows that-

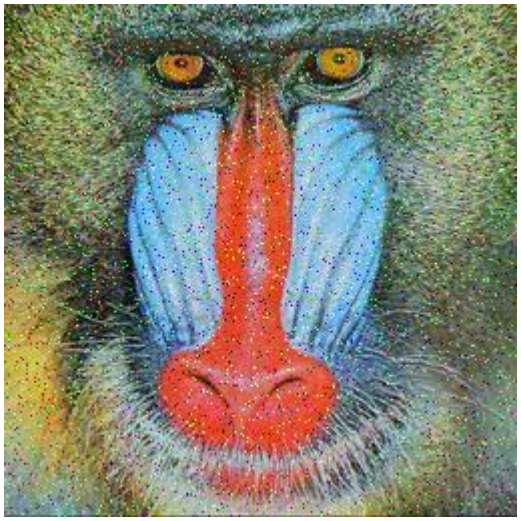
iii) For QR image watermarking there are no difference between the 3 input channels. As a difference outputs are showing one frequency shift and one more peak. Means that the histogram is showing output images are more intense and brighter than the input ones.

Fig 37: Histogram of Baboon image (for both input and output blocks using block division method)

Fig 38: Histogram of input and Output QR image using block division method)

For Block division method Fig 35 shows the histogram of input and output baboon image. There is no significant difference in Histogram which means both images have same quality.

i) In Fig36 histogram of input and output QR images is shown. It shows lesser number of peaks in output image which means output image is compressed.



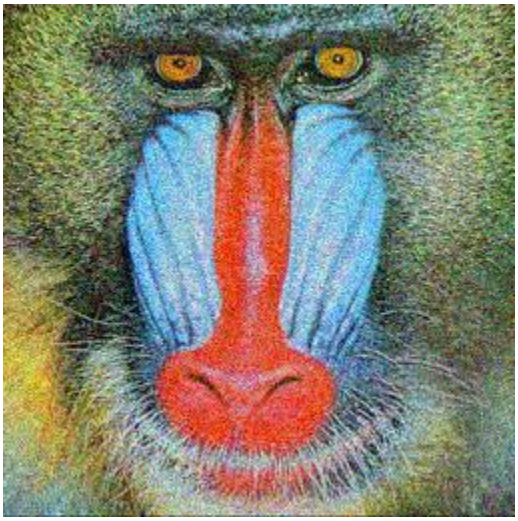
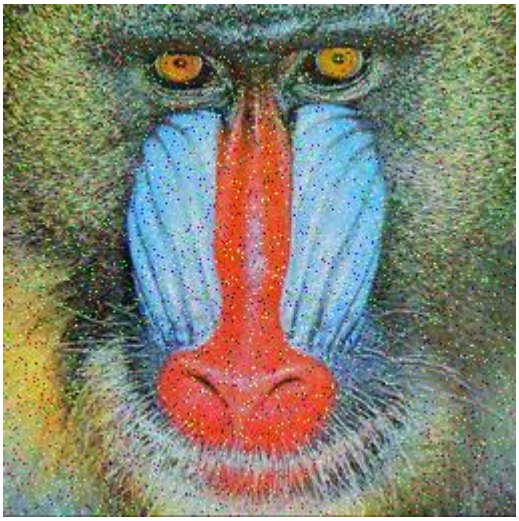


Fig 39: Effect of Salt and pepper and Gaussian Noise in Original image Using Channel separation method



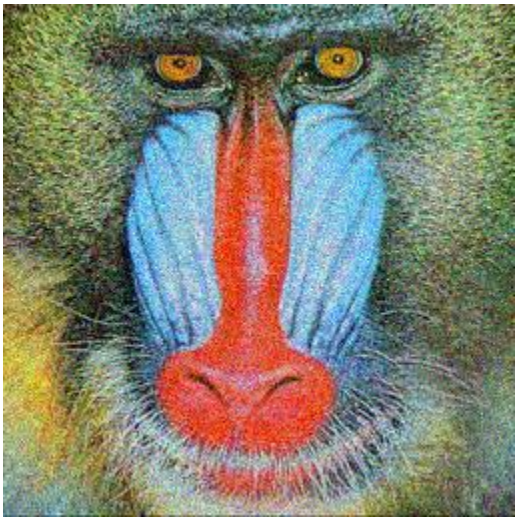


Fig 40: Effect of Salt and pepper and Gaussian Noise in Watermarked image Using Channel separation method

Fig41: Effect of Salt and pepper and Gaussian noise in Host QR image of channel separation method

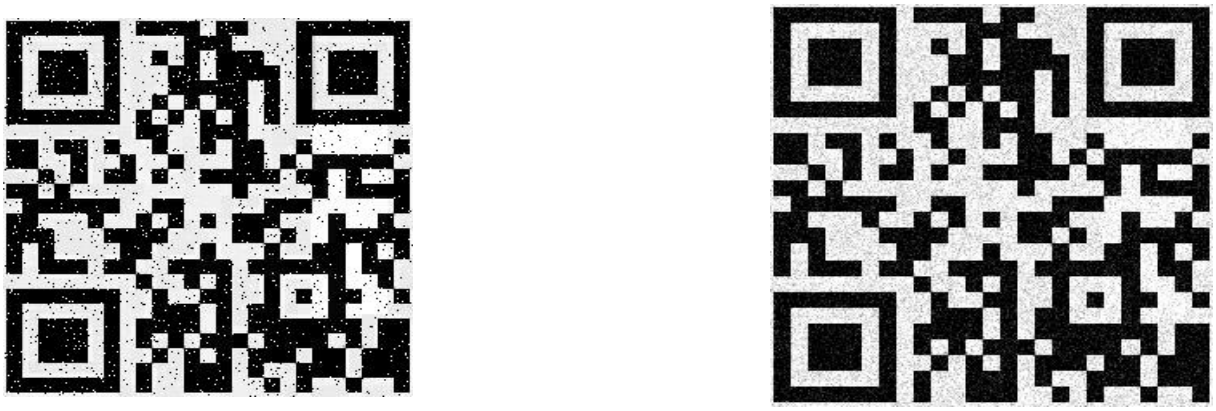


Fig 42: Effect of Salt and pepper and Gaussian noise in Watermarked QR image of channel separation method

Fig 37-38 shows salt and pepper and Gaussian noise applied on both original and watermarked baboon image, No significant visual change is noted. As the watermark cannot extracted properly so the effect of noise in watermark could not discussed.
For figure 39 and 40 there also no significant change is noted.

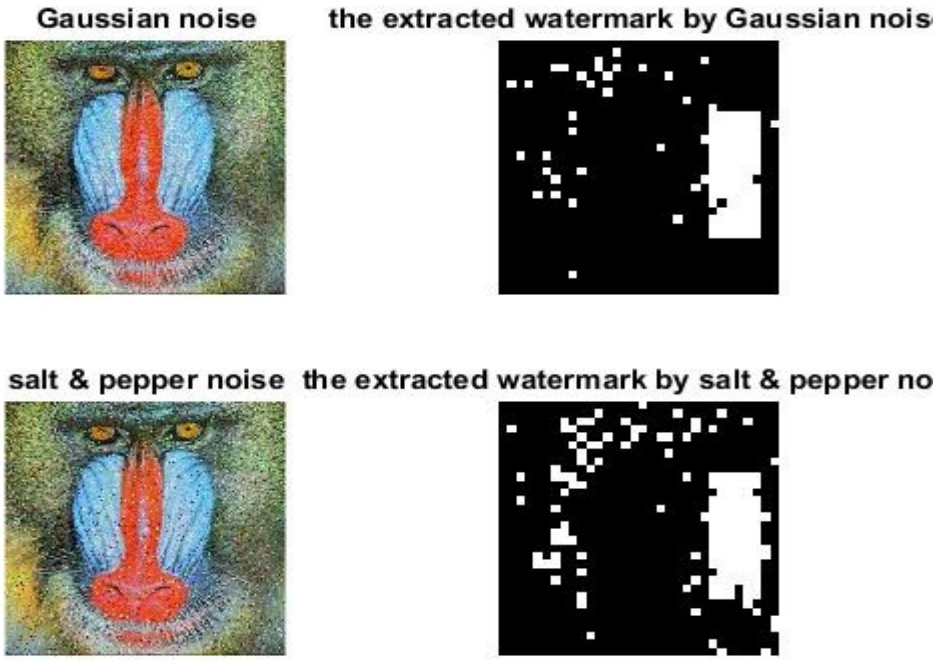


Fig 43: Noise attack on Baboon image using Block division methods

Fig 44: Noise attack on Baboon image using Block division methods

Figure 39 and 41 shows noise effect on both baboon and QR image respectively. It can be stated that this method shows better protection in normal image watermark. The noise is not affecting

the watermark and it can be extracted properly. In case of figure 44 thought the watermarked image is not showing any significant change but the noise destroy the watermark properly.

Remaining Noise of both Methods: Comparison between both methods noise is shown through 1x5 columns, Figure 43 shows effect of Noise attacks on Baboon image using DCT Channel separation method. Where in Table 2 shows the value of Image after noise attack. Figure 43-44 shows the effect of Noise on Watermarked image using Block division method. Table 6 shows value of remaining noise on watermarked image. If comparison is done according to the table, no major difference is found between both methods.

Table 5: For Channel method: (Gaussian Noise)

2.5200	2.5200	2.4807	2.5405	2.5413

Table 6: For Block method: (Gaussian Noise)

2.5200	2.5210	2.4802	2.5400	2.5403

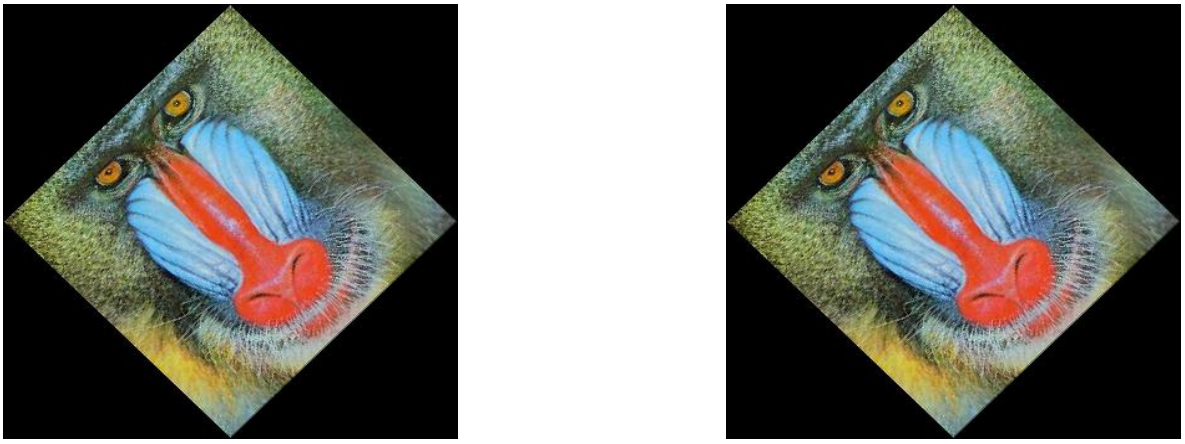


Fig 45: Rotated QR Image Using channel separation method

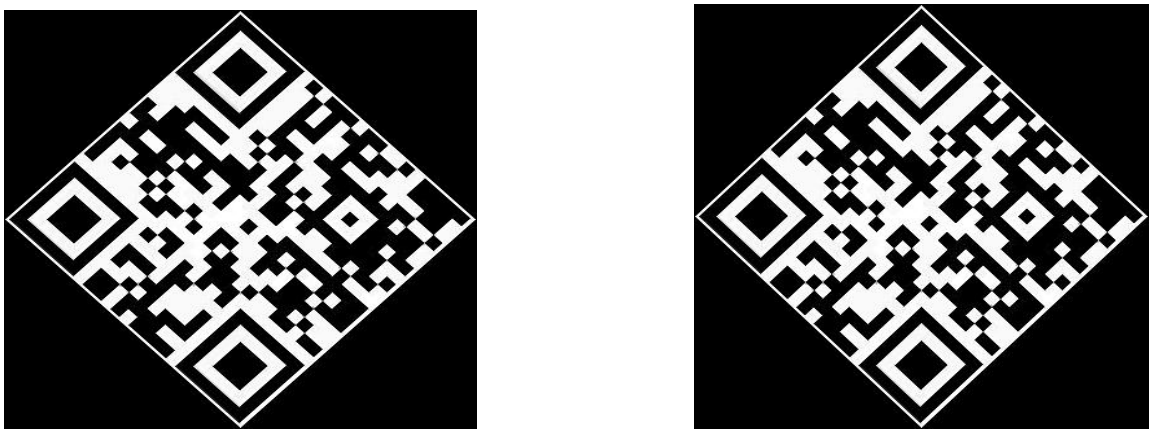


Fig 46: Rotated QR Image Using channel separation method

In Figure 45 and 46 rotation attack is applied both in Original and watermarked image (Normal and QR) and again it does not affect the result

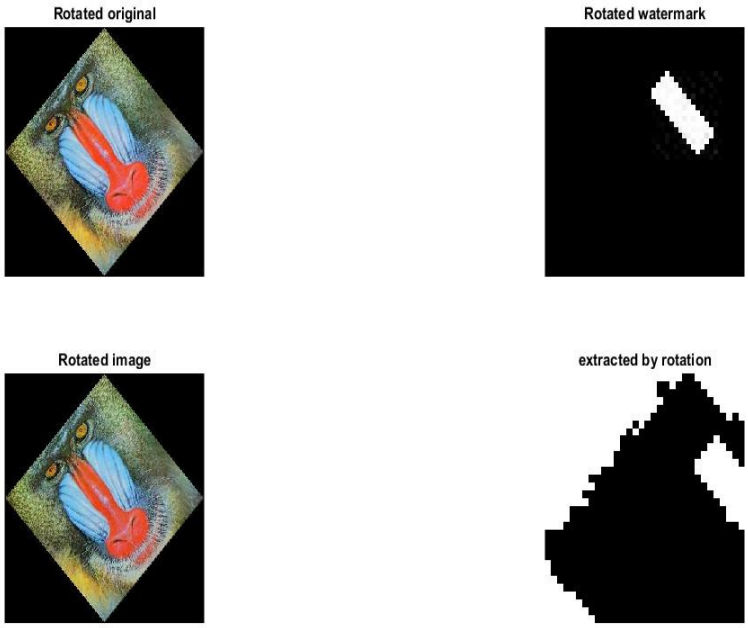


Fig 47: Rotation attack on Baboon image using block division method

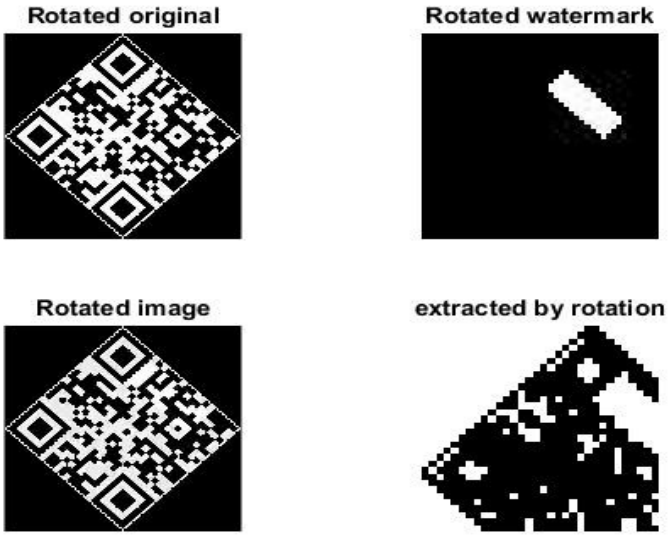


Fig 48: Rotation attack on QR image using block division method

Figure 45 and 46 shows rotation effect on Block division method and it shows the better result for image watermarking and good for QR image rotation. It shows the rotated version of normal embedding and extraction as fig 30 and fig 32.

Overall Discussion:

Pros of Channel separation method:

a) So many attacks have been applied upon the watermarked image using channel separation technique. No visible change is found on it. The watermarking process is then considered as perceptually invisible.
b) Monitoring upon each and every step can be done. The embedding and extraction can be seen step by step
c) It is quite simpler than any other algorithm using DCT.
d) Though its visibility depends upon the embedding strength but choosing correct embedding strength will results in excellent watermarked data.
e) Watermark can be removed completely

Cons of channel separation method:

a) In this method extracted watermark image will not visible to the decoder. So the question might be raised that how it can be understand that the image is watermarked or not?? By comparing the matrix value and histogram matching it can answered.
b) As each and every step of embedding and extraction is monitored it became quite lengthy process.
c) This method will show some visible effects in the upper left corner of normal color image if the embedding strength co- efficient is not choosen properly. It shows robustness against all the attacks in case of QR image watermarking.

Pros of Block division method:

a) Block division method is showing excellent correctness in both cases of embedding and extracting watermarks in normal color images.
b) As DCT is applied to each and every block of the cover image it shows robustness against various compression and noise attacks
c) Watermark image will visible completely after extraction so that we can compare the variations and it shows the best result than any other algorithm

Cons of Block division method:

a) Block size and dividing the host image in non-convergent image block might be a lengthy process some time

b) In case of QR image watermarking it couldn't show the best result as normal image watermarking. Like watermark is slightly visible in embedded QR image.
c) In case of QR image watermark recover 100% like the normal image watermarking.
d) It will not show the intermediate steps of watermarking with an equivalent output image
e) It is not better for noise attack on of QR image.

Conclusion

In this study, the two algorithms DCT channel separation method and DCT Block division methods both the methods have been compared and it has been analyzed that both methods have some limitation and some advantages. As per the study same result has been found for both baboon image and QR image in watermarking process. A good robust watermarked image is achieved by this technique. In case of block division method the result is better for baboon image than QR image. In case of noise attack the watermark is completely distorted. If only embedding of watermark is considered then channel separation method is better in both cases. The drawback in channel separation method is that changes in watermark cannot observed after extraction only the difference images can be shown. No significant changes have been observed in the watermarked image after added different types of attacks (noise, rotation). Block division method has been used for embedding and extraction of watermark and it has showed that better result for baboon image than Channel separation method and same result for QR image. Only drawback of Block division method is that watermark cannot be extracted after only the noise attack (Gaussian noise , Salt and Pepper noise). In this study , it has been observed that channel separation method is good for watermark embedding and prevent attacks. On the other hand the block division method is better for watermark extraction after added some attacks except noise attack for both images. Each of these methods has its advantages and disadvantages, and each one trades some important watermarking property for another.

Future Work

For future research watermarking and QR-code may be developed is to address some of the attacks on the digital document and embedding multimedia(text, image,audio and video) such as Unauthorized Embedding, Unauthorized detection, Unauthorized Removal, and System Attack.

References

1. Zhang Y., "Digital Watermarking Technology: A Review*," ETP International Conference on Future Computer and Communication,* pp. 250-252,2009
2. Mistry D.," Comparison of Digital Water Marking methods" ,(IJCSE) International Journal on Computer Science and Engineering Vol. 02(09), pp 2905-2909,2010
3. Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom," Watermarking applications and their properties", International. Conference on Information Technology 2000
4. Jian sheng M., Sukang L. and Xiaomei Tan, "A Digital Watermarking Algorithm Based On DCT and DWT" , Proceedings of the International Symposium on Web Information Systems and Applications, pp. 104-107,2009
5. Kutter M, Bhattacharjee S.K, Ebrahimi.T, "Towards Second Generation Watermarking Schemes" Proceedings of the 6th International Conference on Image Processing,pp 320-323,1999
6. Tierney E, Newe T, Coffey T," Cox's Algorithm: strengths and weaknesses with varying composition digital images",
7. Poonam, Sharma A, "DCT & DWT based Digital Image Watermarking using Matlab", International Research Journal of Engineering and Technology (IRJET), Vol 03(08),2016
8. Potdar V M., Han S., Chang E." A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics, pp-709-716, 2005
9. Saini L., Shrivastava V., "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST),Vol 2 (3), 2014
10. Baisa L. G, R.R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithms", Journal of Emerging Trends in Computing and Information Sciences,Vol 2(1),2010-11
11. Melinos A., "Digital Watermarking", Computer Graphics Forum 35 (1), pp-261-271,2010
12. Podilchuk C. Delp J.E,"Digital watermarking algorithm and application", IEEE SIGNAL PROCESSING MAGAZINE,Vol 4(3)pp-32-36
13. Podilchuk, C.I., Delp, E.J., 2001. Digital watermarking: Algorithms and applications. IEEE Signal Process. Mag. vol18 (4), 33–46.
14. Anan T,Kuraki K,"Watermarking technology for security enhance documents", FUJITBU BSL tech.J,Vol43(2),pp-197-203,2006
15. Mettripun N, Amornraksa T. "Robust image watermarking based on luminance modification", Journal of Electronic Imaging 22(3), 2013
16. Jimson N, Hemachandran K, "DFT BASED DIGITAL IMAGE WATERMARKING: A SURVEY" Vol 9(2),2018

17. Delaigle J.F, Vleeschouwer C, Macq B.," Watermarking algorithm based on a human visual model", Signal Processing,Vol 5(4)pp-203-204
18. Sheth R,Nath V, "Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method ", Asia Conference on Computer and communication security ,pp 159-172,2018.
19. Yang Y, Li H," The Application of DCT Algorithm in Digital Watermarking by Matlab and Simulation", 7th International Conference on Modelling and identification,Vol3(4) pp 18-20, 2015
20. Solachidis V, Pitas I," Circularly Symmetric Watermark Embedding in 2-D DFT Domain", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10(11), pp-1741-1747, 2001.
21. Agreste S, Andaloro G, "A new approach to pre-processing digital image for wavelet-based watermark", Journal of Computational and Applied Mathematics Vol 221 (08)pp 274–283.2008.
22. Pandey S, Singh P, Pandey V," Block wise image compression & Reduced Blocks Artifacts Using Discrete Cosine Transform", International Journal of Scientific and Research Publications, Vol 5(3), 2015.
23. Barni M, Bartolini F, Cappellini V, Piva A, "A DCT-domain system for robust image watermarking", Signal Processing Vol5 (3) pp-357—372,1998
24. Kuo L,Wei N, "On SVD based watermarking Algorithm" Applied Mathematics and Computation,Vol 188 54–57,2007.
25. Ganic E.,Eskicioglu E," Robust embedding of visual watermarks using discrete wavelet transform and single value decomposition",Journal of Electronic Imaging Vol14(4), 2005
26. Yanyan H,Shuai J, Luo Q, "A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform" Ninth International Conference on P2P,Vol 17(1),2014.
27. Rotation Invariant Digital Image Watermarking Techniques using Zernike Moments and Discrete Cosine Transform ,finalized Thesis work Sodhganga University,2012.
28. Yu L, Niu X , Sun S "Print-and-scan model and the watermarking countermeasure ;Image and Vision Computing "Vol-23 (5) pp-807–814,2005.
29. Lin Y, Yu M,"Rotation scale translation resilient watermarking for images", Transaction on image processing ,vol 10(5),2001.
30. H. S. Kim Y. Baek H. K. Lee "Rotation- scale- and translation-invariant image watermark using higher order spectra" Opt. Eng. vol. 42 (2) pp. 340-349. 2003. "
31. Wang Z. Dong J, Wang W and Tan T , "An Effective watermarking against Valumetric Distortions", December, Volume 14(6,) pp 672–685, 2017.
32. Wua,c,, Zhoub , Xiamu N,"A novel image hash algorithm resistant to print–scan Signal Processing " Vol-89 ,pp2415–2424,2009.
33. J. J. K. O'Ruanaidh T. Pun "Rotation scale and translation invariant spread spectrum digital image watermarking" Signal Processing vol. 66 pp. 303-317 1998.

34. M. Kutter "Watermarking resisting to translation rotation and scaling" Proc. SPIE Multimedia Systems Applications pp. 423-431 1998.
35. Adrian G. Borg Ioannis Pitas,"Image Watermarking Using Dct Domain Constraints "International Journal Of Communications, Vol 3(1), 2009.
36. Lin W, HorngS, Wann K, Fan P," An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization", IEEE TRANSACTIONS ON MULTIMEDIA, Vol. 10(5), 2008.
37. Raymond B. Wolfgang t, Christine I. Podilchuk , and Edward J. Delp "the effect of matching watermark and compression transforms in compressed color images.1998
38. Servetto S, Podilchuk C "Capacity issues for digital watermarking" IEEE Int. Conf. Image Processing '98.
39. Raymond B. Wolfgang, Christine I." Perceptual Watermarks for Digital Images and Video" Proceedings Of The Ieee, VOL. 87 (7),1999.
40. Hui H, Rongxing G, "Research On Watermark Of Electronic Examination Paper" International Symposium on IT,2011
41. Deguillaume F,Voloshynovskiy S,Pun T "Secure hybrid robust watermarking resistant against tampering and copy attack" Proceedings of Signal Processing ,Vol-83 pp 2133–2170.
42. Marshal D.,The Discrete Cosine Transform (DCT),2001.
43. 2-D Discrete cosine transforms
44. Nuno V,"DiscreteCosineTransform Discrete Cosine Transform",
45. Cabeen K. and Peter G, "Image Compression and the Discrete Cosine Transform", Math 45.
46. College of the RedwoodsJuan R, Hernández, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", IEEE TRANSACTIONS ON IMAGE PROCESSING, Vol.9 1, 2000.
47. Saeed K. A., Ahmad R.,Nilchi N, "Robust Digital Image Watermarking Based on Joint DWT-DCT "International Journal of Digital Content Technology and its Applications Volume 3(2), 2009.
48. Jonathan K. Su, Frank Hartung, and Bernd Girod,"A channel Model for watermark attack",Proceedings of Security and Watermarking of Multimedia Contents,Vol-3657.
49. Gupta M, Garg A , "Analysis Of Image Compression Algorithm Using DCT "International Journal of Engineering Research and Applications", Vol. 2,(1), pp515-521, 2012,pp.515-521 .
50. Morris T," Image Processing with MATLAB" , Page 2. Available: http://studentnet. cs.manchester.ac.uk/ugt/COMP27112/doc/matlab.pdf [2 June 2014]
51. Ming Z, Dian-G , Sun.H.S, "Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 14.(6), 2005.

52. :ZhangZ, Sun H, Gao S, Jin S, Selfrecovery reversible image watermarking algorithm. PLoS ONE 13(6):e0199143, (2018).
53. Christoph L, Adriaan Li, and George S ,"Practical Fast 1-D Dct Algorithms With 11 Multiplications," 2006.
54. Khayam S The Discrete Cosine Transform (DCT):Theory and Application ,2003
55. Obukhov A, Kharlamov A,Discrete Cosine Transform for 8x8 Blocks with CUDA,2008
56. Christian C Clark T," Software Watermarking: Models and Dynamic Embedding, Principles of Programming Languages (POPL '99) Jan. 1999.
57. Rong C, LIU Z, JIANG Y, Zhang Y ," Coding Principle and Implementation of Two-dimensional PDF417 Bar Code" 6th IEEE conference on Industrial Electronics and its application,2011.
58. Soon T.,QR Code, Section three, IJSRC, Vol 05(6),2011
59. Liu Y, Yang J, "Recognition of QR Code with mobile phones," in Chinese Control and Decision Conference (CCDC 2008),2008, pp. 203 –206.
60. Sutheebanjard P, Premchaiswadi W.,QR-Code Generator, 2010 Eighth International Conference on ICT and Knowledge Engineering
61. Barmawi, A.M., Yulianto, F.A.: Watermarking QR code. In: 2015 2nd International Conference on Information Science and Security (ICISS), pp. 1–4. IEEE (2015).
62. Li Li, Wang Rui-ling. A digital watermarking algorithm for QR code [J]. Journal of Hangzhou Dianzi. University, 2011, 31(2): 46-49 (in Chinese).
63. Zhou, J & Liu Y & Li P. Research on binarization of QR code image," in Proc. ICMT, 2010, pp. 1–4.
64. Gu Y, Zhang W. "QR code recognition based on image processing." International Conference on Information Science and Technology *): 733-736, 2011*.
65. Sartid V, "QR Code Using Invisible Watermarking in Frequency Domain" Ninth International Conference on ICT and Knowledge Engineering,, pp. 47-52, 2012.
66. RouA-L Yuan F, Ying G,"QR code image detection using run-length coding ,Proc. ICCSNT, Harbin, China,2130–2134, 2011.
67. Jun-Chou Chuang, Yu-Chen Hu & Hsien-Ju Ko. A Novel Secret Sharing Technique Using QR Code, International,Journal of Image Processing (IJIP), Volume (4) : Issue (5), pp. 468-475, 2010.
68. M. F. I. Kamil and K. A. Jalil, "The embedding of Arabic characters in QR code," 2012 in IEEE Conference on Open Systems, pp. 1–5, 2012.
69. Ming Sun , Jibo Si & Shuhuai Zhang , "Research on embedding and extracting methods for digital watermarks applied to QR code images", New Zealand Journal of Agricultural Research, 50:5, 861-867.
70. Thulasidharan P and Nair. M. S. ,"QR code based blind digital image watermarking with attack detection code." International Journal of Electronics and Communications, 69(7):1074 – 1084, 2015.

71. Gonzalo J. Garateguy, Gonzalo R. Daniel L. Lau,and Ofelia P. Villarreal,QR Images: Optimized Image Embedding in QR Codes", VOL. 23(7), 2014.

72. Suwito M et al., "Integrity Watermarking and QR-Code Techniques for ensuring Printed Document Authenticity Real Time Distribution"
73. Nesson, C. Encoding multi-layered data into QR codes for increased capacity and security. Diss. South Dakota School of Mines and Technology, 2013.
74. Gaikwad A, "Embedding QR Code in Color Images using Halftoning Technique" International Journal of science and research,Vol-8(2),2008.
75. Saraswati M, Maroti M, Sainath M, Prakash S,"QR Code Watermarking Algorithm Based on DWT and Counterlet Transform for Authentication" Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1233-1244 .
76. Shaikh H, Imran M, Kelkar Y, "A Robust DWT Digital Image Watermarking Technique Basis On Scaling Factor" International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2(4)2012.
77. Mishra A., Agarwal Charu, Chetty G "Optimization of Scaling Factors for Image Watermarking Using Harmony Search Algorithm" International Journal Of Engineering And Computer Science Volume – 3(8) ,7776-7782, 2014.
78. Pandey S, Singh M.P, Pandey V,"Block wise image compression & Reduced Blocks Artifacts Using Discrete Cosine Transform" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 11(.2) 2002.

Appendix

i. Color Image watermarking using channel separation method:

```
close all
x=double(imread('C:\Users\ISHITA\Documents\MATLAB\baboon c.jpg'));
figure(1);imshow(x/255);
title ('original image');
y=x;
a=zeros(300,500);
a(100:250,100:350)=1;
figure(2);imshow(a)
title ('watermark')
save ('C:\Users\ISHITA\Documents\MATLAB\m.dat','a','-ascii');
%%
% %watermarking
x1=x(:,:,1);
x2=x(:,:,2);
x3=x(:,:,3);
dx1=dct2(x1);dx11=dx1;
dx2=dct2(x2);dx22=dx2;
dx3=dct2(x3);dx33=dx3;
% figure(3);imshow (dx1);
% figure(4);imshow (dx2);
% figure(5);imshow (dx3);
loadm.dat
g=2;%co -efficient of watermark strength
[rm,cm]=size(m);
dx1(1:rm,1:cm)=dx1(1:rm,1:cm)+g*m;
dx2(1:rm,1:cm)=dx2(1:rm,1:cm)+g*m;
dx3(1:rm,1:cm)=dx3(1:rm,1:cm)+g*m;
% figure(6); imshow(dx1);
% figure(7); imshow(dx2);
% figure(8); imshow(dx3);
y1=idct2(dx1);
y2=idct2(dx2);
y3=idct2(dx3);
y(:,:,1)=y1;
y(:,:,2)=y2;
```

```
y(:,:,3)=y3;
figure(9);imshow(y);
figure(10);imshow(y/255);
title ('watermarked image');
figure(11);imshow(abs(y-x)*100);
z=y;
[r,c,s]=size(z);
% De watermarking
% clean image(known mask)
y=z;
dy1=dct2(y(:,:,1));
dy2=dct2(y(:,:,2));
dy3=dct2(y(:,:,3));
dy1(1:rm,1:cm)=dy1(1:rm,1:cm)-g*m;
dy2(1:rm,1:cm)=dy2(1:rm,1:cm)-g*m;
dy3(1:rm,1:cm)=dy3(1:rm,1:cm)-g*m;
y11=idct2(dy1);
y22=idct2(dy2);
y33=idct2(dy3);
yy(:,:,1)=y11;
yy(:,:,2)=y22;
yy(:,:,3)=y33;
figure(12);imshow(y11);
figure(13);imshow(y22);
figure(14);imshow(y33);
figure(15); imshow(yy/255);
figure(16);imshow(abs(yy-x)*1000);
```

ii.Color Image watermarking using Block division method:

```
M=256; %the length of the original image
N=32; %the length of the watermark image
K=8;
V=zeros(K,K);
 HI=imread('C:\Users\ISHITA\Documents\MATLAB\Baboon.jpeg');
 I=HI;
subplot(2,2,1);
```

```
imshow(I); %display the original image
title('the original image');
 J=zeros(32,32);
J(10:25,25:30)=1;
subplot(2,2,2);
imshow(J);%display the watermark image
title('the watermark image');

% embedding watermark
for p=1:N
for q=1:N
       x=(p-1)*K+1;
       y=(q-1)*K+1;
       V=I(x:x+K-1,y:y+K-1);
       V1=dct2(V);
if J(p,q)==0
          a=-1;
else a=1;
end
V1(1,1)=V1(1,1)*(1+a*0.06);
V2=idct2(V1);
I(x:x+K-1,y:y+K-1)=V2;
end
end
subplot(2,2,3);
imshow(I);%display the watermarked image
title('the watermarked image')
imwrite(I,'C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage.jpeg');
%withdraw watermark
 B1=zeros(K,K);
 B2=zeros(K,K);
 I1=imread('C:\Users\ISHITA\Documents\MATLAB\Baboon.jpeg');
 J1=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage.jpeg');
for p=1:N
for q=1:N
       x=(p-1)*K+1;
       y=(q-1)*K+1;
       B1=I1(x:x+K-1,y:y+K-1);
       B2=J1(x:x+K-1,y:y+K-1);
       B1=idct2(B1);
```

```
        B2=idct2(B2);
        a=B2(1,1)/B1(1,1)-1;
if a<0
W(p,q)=0;
else
W(p,q)=1;
end
end
end
subplot(2,2,4);
imshow(W); %display the withdraw watermark image
title('extracted watermark');
```

iii.QR image watermarking using channel separation method:

```
closeall
% subplot (2,2,1)
x=double(imread('C:\Users\ISHITA\Documents\MATLAB\demoQR 1new.jpg'));
figure(1),imshow(x/255);
title ('original QR image');
y=x;
% subplot(2,2,2)
a=zeros(150,150);
a(75:90,75:100)=1;
figure(2),imshow(a);
title ('watermark')
save ('C:\Users\ISHITA\Documents\MATLAB\m.dat','a','-ascii');
%watermarking
X1=y(:,:,1);
X2=y(:,:,2);
X3=y(:,:,3);
%%steps for dct2 conversion
result1=padarray(X1,[2,2],2,'both');
result2=padarray(X2,[2,2],2,'both');
result3=padarray(X3,[2,2],2,'both');
P1=dct(result1);
P2=dct(result2);
```

```
P3=dct(result3);
D1=transpose(P1);
D2=transpose(P2);
D3=transpose(P3);
W1=dct(D1);
W2=dct(D2);
W3=dct(D3);
I1=transpose(W1);
I2=transpose(W2);
I3=transpose(W3);
figure(3);imshow (I1);
figure(4);imshow(I2);
figure(5);imshow (I3);
loadm.dat
g=10;
[rm,cm]=size(m);
I1(1:rm,1:cm)=I1(1:rm,1:cm)+g*m;
I2(1:rm,1:cm)=I2(1:rm,1:cm)+g*m;
I3(1:rm,1:cm)=I3(1:rm,1:cm)+g*m;
figure(6); imshow(I1);
figure(7); imshow(I2);
figure(8); imshow(I3);
%steps for idct2 conversion
z1=idct(I1);
z2=idct(I2);
z3=idct(I3);
E1=transpose(z1);
E2=transpose(z2);
E3=transpose(z3);
D1=idct(E1);
D2=idct(E2);
D3=idct(E3);
r1=transpose(D1);
r2=transpose(D2);
r3=transpose(D3);
figure(9),imshow(r1);
figure(10),imshow(r2);
figure(11),imshow(r3);
A1=r1(2+1:end-2,2+1:end-2);
A2=r2(2+1:end-2,2+1:end-2);
```

```
A3=r3(2+1:end-2,2+1:end-2);
y(:,:,1)=A1;
y(:,:,2)=A2;
y(:,:,3)=A3;
% subplot (2,2,3);
figure(12),imshow(y);
figure(13);imshow(y/255);
title ('watermarked image')
figure(14);imshow(abs(y-x)*100);% shows the absolute difference between two images
title ('diff.of original and watermarked image');
t=y;
[r,c,s]=size(t);
% De watermarking
J1=y(:,:,1);
J2=y(:,:,2);
J3=y(:,:,3);
Q1=padarray(J1,[2,2],2,'both');
Q2=padarray(J2,[2,2],2,'both');
Q3=padarray(J3,[2,2],2,'both');
S1=dct(Q1);
S2=dct(Q2);
S3=dct(Q3);
V1=transpose(S1);
V2=transpose(S2);
V3=transpose(S3);
M1=dct(V1);
M2=dct(V2);
M3=dct(V3);
J1=transpose(M1);
J2=transpose(M2);
J3=transpose(M3);
J1(1:rm,1:cm)=J1(1:rm,1:cm)-g*m;
J2(1:rm,1:cm)=J2(1:rm,1:cm)-g*m;
J3(1:rm,1:cm)=J3(1:rm,1:cm)-g*m;
y11=idct(J1);
y22=idct(J2);
y33=idct(J3);
V11=transpose(y11);
V22=transpose(y22);
V33=transpose(y33);
```

```
M11=idct(V11);
M22=idct(V22);
M33=idct(V33);
J11=transpose(M11);
J22=transpose(M22);
J33=transpose(M33);
B1=J11(2+1:end-2,2+1:end-2);
B2=J22(2+1:end-2,2+1:end-2);
B3=J33(2+1:end-2,2+1:end-2);
yy(:,:,1)=B1;
yy(:,:,2)=B2;
yy(:,:,3)=B3;
figure(15); imshow(yy/255);
title ('De-watermarked cover image');
figure(16);imshow(abs(yy-x)*1000);
title ('diff.of original and dewatermarked image');
```

i. QR image watermarking using block division method:

```
M=256; %the length of the original image
N=32; %the length of the watermark image
K=8;
V=zeros(K,K);
 HI=imread('C:\Users\ISHITA\Documents\MATLAB\download.jpg');
 I=HI;
subplot(2,2,1);
imshow(I); %display the original image
title('the original image');

 J=zeros(32,32);
J(10:25,25:30)=1;
subplot(2,2,2);
imshow(J);%display the watermark image
title('the watermark image');

% embedding watermark
for p=1:N
for q=1:N
      x=(p-1)*K+1;
```

```
        y=(q-1)*K+1;
        V=I(x:x+K-1,y:y+K-1);
        V1=dct2(V);
if J(p,q)==0
            a=-1;
else a=1;
end
V1(1,1)=V1(1,1)*(1+a*0.06);
V2=idct2(V1);
I(x:x+K-1,y:y+K-1)=V2;
end
end
subplot(2,2,3);
imshow(I);%display the watermarked image
title('the watermarked image')
imwrite(I,'C:\Users\ISHITA\Documents\MATLAB\WatermarkedQR.jpg');
%withdraw watermark
 B1=zeros(K,K);
 B2=zeros(K,K);
 I1=imread('C:\Users\ISHITA\Documents\MATLAB\download.jpg');
 J1=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedQR.jpg');
for p=1:N
for q=1:N
        x=(p-1)*K+1;
        y=(q-1)*K+1;
        B1=I1(x:x+K-1,y:y+K-1);
        B2=J1(x:x+K-1,y:y+K-1);
        B1=idct2(B1);
        B2=idct2(B2);
        a=B2(1,1)/B1(1,1)-1;
if a<0
W(p,q)=0;
else
W(p,q)=1;
end
end
end
subplot(2,2,4);
imshow(W); %display the withdraw watermark image
title('extracted watermark');
```

v. Attacks on normal image watermarking in Channel separation methods:

a. Noise attacks

b. Rotation scaling attacks

vi. Attacks on QR image watermarking in Channel separation method:

a. Noise attacks:

```
b. NT1=imnoise((y/255),'gaussian');
c. figure(19);imshow(NT1);
d. cc=(abs(NT1-x)*100);
e. imshow(cc);
f. NT2=imnoise((y/255),'salt & pepper');
g. figure(90);imshow(NT2-(x)*100);
h.  NT3=imnoise((G),'speckle');
i.  figure(21);imshow(NT3);
j.
```

k. Rotation scaling attacks

```
l. % LL=imrotate((y),60);
m. %  figure(17);imshow(LL-(y));
n. DD=imresize((y/255),2.5);
o. figure(18);imshow(DD);
p. % FF=imresize(x,2.5);
q. % imshow(abs(DD-FF)*1000);
r.
```

vii. Attacks on Normal image watermarking in block division method:

a. Noise attacks:

```
M=256;
N=32;
K=8;
D=zeros(M,M);
```

```
BLOCK1=zeros(K,K);
BLOCK2=zeros(K,K);
QI=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage.jpeg');
S=QI;
G=imnoise(S,'gaussian');
imwrite(G,'C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage1.jpeg');
A=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage1.jpeg');
subplot(2,2,1);
imshow(A);
title('Gaussian noise');
J=imnoise(S,'salt& pepper');
imwrite(J,'C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage2.jpeg');
B=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage2.jpeg');
subplot(2,2,3);
imshow(B);
title('salt & pepper noise');
I=imread('C:\Users\ISHITA\Documents\MATLAB\Baboon.jpeg');
for p=1:N
for q=1:N
      x=(p-1)*K+1;
      y=(q-1)*K+1;
      BLOCK1=I(x:x+K-1,y:y+K-1);
      BLOCK2=A(x:x+K-1,y:y+K-1);
      BLOCK1=idct2(BLOCK1);
      BLOCK2=idct2(BLOCK2);
      a=BLOCK2(1,1)/BLOCK1(1,1)-1;
if a<0
W(p,q)=0;
else
W(p,q)=1;
end
end
end
subplot(2,2,2);
imshow(W);%display the extracted watermark
title('the extracted watermark by Gaussian noise');
I=imread('C:\Users\ISHITA\Documents\MATLAB\Baboon.jpeg');
B=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage2.jpeg');
for p=1:N
for q=1:N
```

```
        x=(p-1)*K+1;
        y=(q-1)*K+1;
BLOCK1=I(x:x+K-1,y:y+K-1);
BLOCK2=B(x:x+K-1,y:y+K-1);
BLOCK1=idct2(BLOCK1);
BLOCK2=idct2(BLOCK2);
a=BLOCK2(1,1)/BLOCK1(1,1)-1;
if a<0
W(p,q)=0;
else W(p,q)=1;
end
end
end
subplot(2,2,4);
imshow(W);%display the extracted watermark
title('the extracted watermark by salt & pepper noise');
```

b. Rotation and scaling attacks:

```
M=256;
N=32;
K=8;
D=zeros(M,M);
BLOCK1=zeros(K,K);
BLOCK2=zeros(K,K);
AI=imread('C:\Users\ISHITA\Documents\MATLAB\Baboon.jpeg');
X=AI;
R1=imrotate(X,45);
imwrite(R1,'C:\Users\ISHITA\Documents\MATLAB\rotatedB.jpeg');
V1=imread('C:\Users\ISHITA\Documents\MATLAB\rotatedB.jpeg');
subplot (2,2,1);
imshow (V1);
title('Rotated original');
 J=zeros(32,32);
J(10:25,25:30)=1;
ff=J;
 R2=imrotate(ff,45);
imwrite(R2,'C:\Users\ISHITA\Documents\MATLAB\Rotated wm.jpg');
g1=imread('C:\Users\ISHITA\Documents\MATLAB\Rotated wm.jpg');

subplot (2,2,2);
```

```
imshow(g1);
title ('Rotated watermark');
QI=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImage.jpeg');
S=QI;
R2=imrotate(S,45);
imwrite(R2,'C:\Users\ISHITA\Documents\MATLAB\Rotated image.jpeg');
V2=imread('C:\Users\ISHITA\Documents\MATLAB\Rotated image.jpeg');
subplot (2,2,3);
imshow (V2);
title('Rotated image');
for p=1:N
for q=1:N
      x=(p-1)*K+1;
      y=(q-1)*K+1;
BLOCK1=V1(x:x+K-1,y:y+K-1);
BLOCK2=V2(x:x+K-1,y:y+K-1);
BLOCK1=idct2(BLOCK1);
BLOCK2=idct2(BLOCK2);
a=BLOCK2(1,1)/BLOCK1(1,1)-1;
if a<0
W(p,q)=0;
else W(p,q)=1;
end
end
end
subplot (2,2,4);
imshow (W);
title ('extracted by rotation');
```

viii. Attacks on QR image watermarking in block division method:

a. Noise attacks on QR image:

```
M=256;
N=32;
K=8;
D=zeros(M,M);
BLOCK1=zeros(K,K);
BLOCK2=zeros(K,K);
QI=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedQR.jpg');
```

```
S=QI;
G=imnoise(S,'gaussian');
imwrite(G,'C:\Users\ISHITA\Documents\MATLAB\WatermarkedImageQR1.jpg');
A=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImageQR1.jpg');
subplot(2,2,1);
imshow(A);
title('Gaussian noise');
J=imnoise(S,'salt& pepper');
imwrite(J,'C:\Users\ISHITA\Documents\MATLAB\WatermarkedImageQR2.jpg');
B=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImageQR2.jpg');
subplot(2,2,3);
imshow(B);
title('salt & pepper noise');
I=imread('C:\Users\ISHITA\Documents\MATLAB\download.jpg');
for p=1:N
for q=1:N
      x=(p-1)*K+1;
      y=(q-1)*K+1;
      BLOCK1=I(x:x+K-1,y:y+K-1);
      BLOCK2=A(x:x+K-1,y:y+K-1);
      BLOCK1=idct2(BLOCK1);
      BLOCK2=idct2(BLOCK2);
      a=BLOCK2(1,1)/BLOCK1(1,1)-1;
if a<0
W(p,q)=0;
else
W(p,q)=1;
end
end
end
subplot(2,2,2);
imshow(W);%display the extracted watermark
title('the extracted watermark by Gaussian noise');
I=imread('C:\Users\ISHITA\Documents\MATLAB\Download.jpg');
B=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedImageQR2.jpg');
for p=1:N
for q=1:N
      x=(p-1)*K+1;
      y=(q-1)*K+1;
BLOCK1=I(x:x+K-1,y:y+K-1);
```

```
BLOCK2=B(x:x+K-1,y:y+K-1);
BLOCK1=idct2(BLOCK1);
BLOCK2=idct2(BLOCK2);
a=BLOCK2(1,1)/BLOCK1(1,1)-1;
if a<0
W(p,q)=0;
else W(p,q)=1;
end
end
end
subplot(2,2,4);
imshow(W);%display the extracted watermark
title('the extracted watermark by salt & pepper noise');
```

b. Rotation and scaling attacks on QR image:

```
M=256;
N=32;
K=8;
D=zeros(M,M);
BLOCK1=zeros(K,K);
BLOCK2=zeros(K,K);
AI=imread('C:\Users\ISHITA\Documents\MATLAB\download.jpg');
X=AI;
R1=imrotate(X,45);
imwrite(R1,'C:\Users\ISHITA\Documents\MATLAB\rotatedQR.jpg');
V1=imread('C:\Users\ISHITA\Documents\MATLAB\rotatedQR.jpg');
subplot (2,2,1);
imshow (V1);
title('Rotated original');
 J=zeros(32,32);
J(10:25,25:30)=1;
kk=J;
  L=imrotate(kk,45);
imwrite(L,'C:\Users\ISHITA\Documents\MATLAB\Rotatedwm1.jpg');
g1=imread('C:\Users\ISHITA\Documents\MATLAB\Rotatedwm1.jpg');
subplot (2,2,2);
imshow(g1);
title ('Rotated watermark');
QI=imread('C:\Users\ISHITA\Documents\MATLAB\WatermarkedQR.jpg');
```

```
S=QI;
R2=imrotate(S,45);
imwrite(R2,'C:\Users\ISHITA\Documents\MATLAB\RotatedQRwm.jpg');
V2=imread('C:\Users\ISHITA\Documents\MATLAB\RotatedQRwm.jpg');
subplot (2,2,3);
imshow (V2);
title('Rotated image');
for p=1:N
for q=1:N
      x=(p-1)*K+1;
      y=(q-1)*K+1;
BLOCK1=V1(x:x+K-1,y:y+K-1);
BLOCK2=V2(x:x+K-1,y:y+K-1);
BLOCK1=idct2(BLOCK1);
BLOCK2=idct2(BLOCK2);
a=BLOCK2(1,1)/BLOCK1(1,1)-1;
if a<0
W(p,q)=0;
else W(p,q)=1;
end
end
end
subplot (2,2,4);
imshow (W);
title ('extracted by rotation');
```